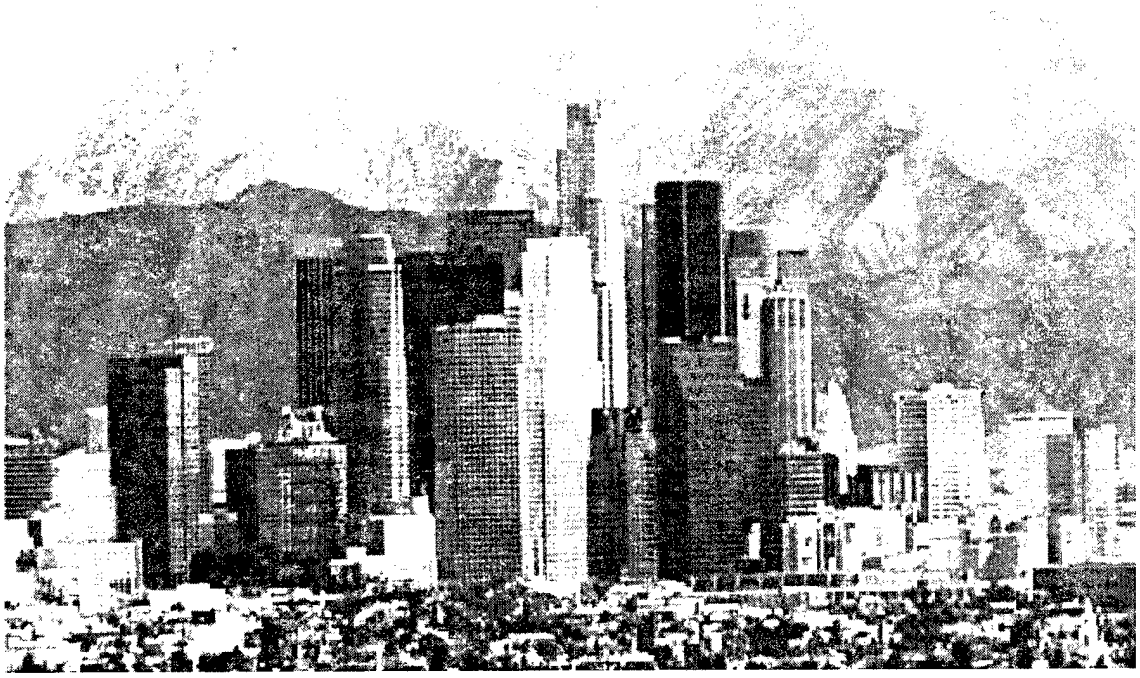
DOCUMENTED BRIEFING

Security and Safety in Los Angeles High-Rise Buildings After 9/11

Rae W. Archibald, Jamison Jo Medby, Brian Rosen, Jonathan Schachter



RAND Public Safety and Justice

DOCUMENTED BRIEFING

Security and Safety in Los Angeles High-Rise Buildings After 9/11

Rae W. Archibald, Jamison Jo Medby, Brian Rosen, Jonathan Schachter

Prepared for the Building Owners and
Managers Association of Greater Los Angeles (BOMA)

RAND Public Safety and Justice

The research described in this report was prepared for the Building Owners and Managers Association of Greater Los Angeles (BOMA).

ISBN: 0-8330-3184-8

The RAND documented briefing series is a mechanism for timely, easy-to-read reporting of research that has been briefed to the client and possibly to other audiences. Although documented briefings have been formally reviewed, they are not expected to be comprehensive or definitive. In many cases, they represent interim work.

Published 2002 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 102, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Email: order@rand.org

Preface

RAND

There are approximately 43 million square feet of commercial and retail space in the 65 block area in the core of downtown Los Angeles encompassed by the Downtown Center Business Improvement District. Ten buildings contain more that 1 million square feet each (about 12 million square feet total), and each of those buildings houses around 4,100 occupants. All told, there are some 18 buildings over 500 feet tall in the downtown Los Angeles core and one building over 1,000 feet tall. The Downtown Center Business Improvement District estimates there are about 145,000 workers in this area. This estimate does not count tourists, vendors, or others who come to the area to conduct business. On a busy work day, it would be fair to suggest that perhaps 200,000 people would be in the downtown core.

This density of population and buildings, with its concentration of high-rise buildings, provides the motivation for this short analysis of high-rise building security and safety in Los Angeles commissioned by the Building Owners and Managers Association of Greater Los Angeles (BOMA) and conducted by RAND. The idea for the study was initiated by Los Angeles City Attorney Rocky Delgadillo. The results have been briefed to BOMA and the city attorney's office and are available to the public on the web at www.rand.org/publications/DB/DB381.

Acknowledgments

RAND

We are grateful to the leadership of the Building Owners and Managers Association of Greater Los Angeles (BOMA) and Los Angeles City Attorney Rocky Delgadillo for having the vision to see that a short analysis such as this might be useful, and for persevering to raise the money to fund it. Special thanks go to Geoff Ely, former president of BOMA, Martha Cox-Nitikman of the BOMA staff, Ben Austin, formerly of the city attorney's staff, and the leadership of the Los Angeles region of the National Electrical Contractors Association.

We also want to thank the many building owners, managers, security directors and vendors, building staff, consultants, and law enforcement officials who took the time to share with us their operations, ideas for improvement, and comments on earlier drafts of this document. We greatly appreciate the time taken by City Attorney Rocky Delgadillo and his staff to review our work and the participation of many dedicated members of BOMA.

Jack Riley, director of the RAND Public Safety and Justice unit, deserves special thanks for carefully reviewing and improving our work.

Briefing Outline

- √ Introduction and Summary Observations
- Key Considerations for Building Security
  - Defining the threats and vulnerabilities
  - Establishing the objectives of security
  - Understanding existing security practices and technologies
  - A context for existing security measures
- Learning from Three Case Studies
  - Lessons learned from 9/11
  - A best case example: Chicago
  - Indirect economic costs: Closing Pennsylvania Avenue
- Key Planning Considerations for High-Rise Buildings
- Potential Roles for Government
- Recommendations for Los Angeles

RAND

This documented briefing consists of six segments. We begin with the introduction and summary observations.

Introduction

- **9/11 raises many questions about high-rise building security practices in Los Angeles**
- **Building Owners and Managers Association commissioned a short study by RAND at the behest of Los Angeles City Attorney Rocky Delgadillo**
- **Study to be presented as a "documented briefing" for building owners and managers, building occupants, and public officials**
  - **Identify generic threats**
  - **Identify exemplary practices**
  - **Discuss issues after an event**
  - **Suggest potential public policy actions**

RAND

The Building Owners and Managers Association of Greater Los Angeles and the Office of the City Attorney, Rocky Delgadillo, contacted RAND late last fall requesting a short study that would focus on the threats to and possible responses from the owners and managers of Los Angeles high-rise buildings in the aftermath of 9/11. The city attorney's office was also interested in potential public policy changes or programs that government might undertake of facilitate to improve the security and safety of occupants of high-rise buildings in Los Angeles.

Specifically, RAND set out to identify generic threats, identify exemplary practices in Los Angeles and elsewhere (in this case selecting Chicago as an example), discuss potential actions after an event, and suggest potential preparations that local government and the private sector might want to consider.

Given the low cost and relatively short time period for the study, the methodology was straightforward. RAND conducted literature searches, personal and telephone interviews, and group discussions with a wide range of parties interested in and relevant to the safety and security of high-rise buildings. We also conducted some on-site discussions and field observations in downtown Los Angeles.

Finally, we drew upon significant existing RAND resources, including

- staff expertise on the terrorist mindset, technology, and weapons of mass destruction
- recent RAND work on terrorism for the California Office of Emergency Services and the Speaker of the California Assembly, and related work on planning for bioterrorism in Los Angeles County, among others. All of this work influenced us, at least indirectly, even if we have not cited it explicitly.

Because this analysis was conducted while events were moving very rapidly and the Office of Homeland Security was evolving, certain aspects will be outdated in a relatively short time period. However, we have tried to concentrate on those items and issues that can be useful over an extended time period.

Summary Observations

- **Threat conditions**
  - **The possibility that Los Angeles high-rise buildings will be the target of a large-scale incident by international terrorist organizations is real but relatively small compared with other possible targets across the nation**
  - **The threat of bombs, conveyed in a variety of ways, remains real and moderately likely**
  - **The threat of biological or chemical weapons attacks is less likely**

RAND

The terrorist threat cannot be specified with any certainty. However, it is likely that explosive or incendiary devices are a more significant threat currently than chemical, biological, or other weapons of mass destruction.

Summary Observations (continued)

- **Considerations for building owners**
  - **There is little a building owner (public or private) can do to *prevent* the type of catastrophic incident that occurred on 9/11**
    - **Most prevention measures are the responsibility of the federal government**
    - **Intelligence collection efforts can help prevent and/or deter attacks**
      - **Buildings having access to such intelligence can aid in preventing and or deterring attacks**
      - **Communication and coordination with law enforcement and intelligence agencies is critical**
  - **Mitigating the effects of an attack becomes paramount**
    - **Emergency preparedness and response plans can moderate the effects of an attack**

RAND

Most key terrorism *prevention* activities are governmental responsibilities, especially the federal government. The types of prevention steps that building owners can take generally do not address catastrophic terrorist threats. However, building owners can do a great deal to manage and mitigate the consequences of catastrophic attacks.

Summary Observations (continued)

- **The current state of readiness among Los Angeles high-rise buildings in the wake of 9/11**
  - **Most buildings have instituted some form of access control**
  - **Most buildings are assessing surveillance and perimeter security**
  - **Downtown high-rise buildings have added security personnel, some of whom will remain permanently**
  - **Some buildings are attempting to use technology to substitute for increased staff**
  - **A "security standard" has not emerged, but stricter access controls are here to stay**

RAND

We found that most buildings have changed security procedures since 9/11. Although a "security standard" has not emerged, we expect stricter access controls of one type or another to be permanent additions to downtown high-rise buildings.

Summary Observations (continued)

- **Other consequences of a changed security environment**
  - **Access control and perimeter security need to be supplemented**
  - **Emergency preparedness plans should be reviewed and modified, if necessary**
  - **Tenants should receive education and training regarding evacuation procedures and, possibly, how to help identify potential attackers**

RAND

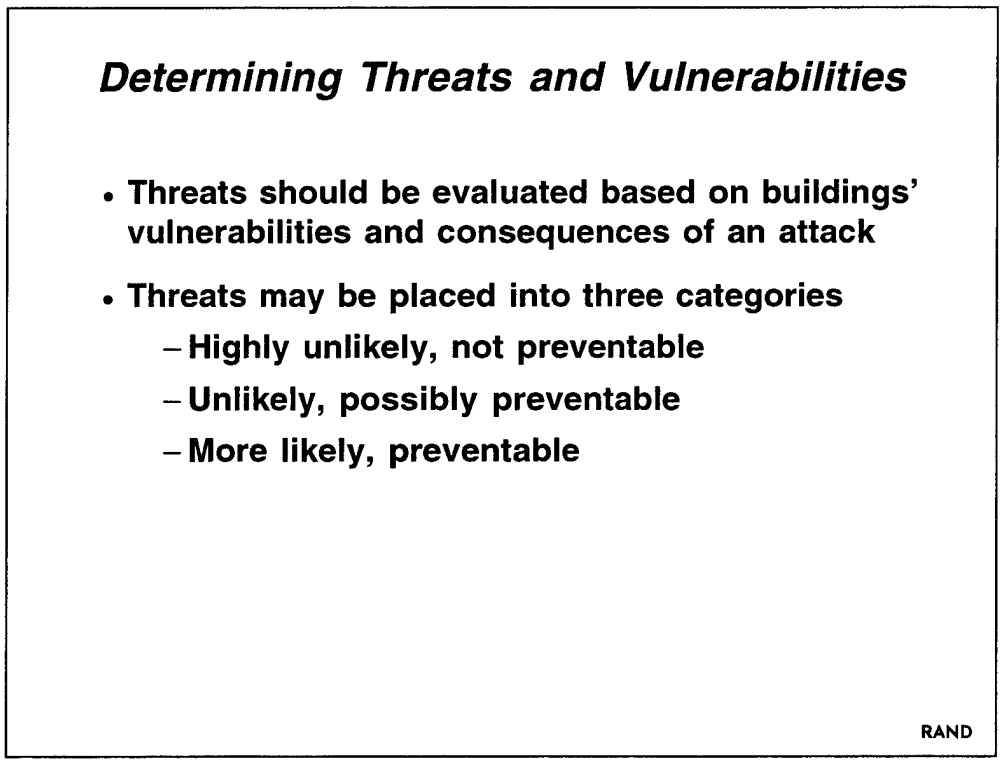
Increased attention to access control and perimeter security are first lines of defense, but emergency preparedness plans and tenant education are likely to prove to be the most important life safer in the event of an attack. Los Angeles has exemplary practices in place for dealing with earthquake and fire threats, but the terrorist threat increases the need for building occupants to be well-trained to respond to an incident. This likely means more practice and more exercises than are currently the norm.

Briefing Outline

- **Introduction and Summary Observations**
- √ **Key Considerations for Building Security**
  - **Defining the threats and vulnerabilities**
  - **Establishing the objectives of security**
  - **Understanding existing security practices and technologies**
  - **A context for existing security measures**
- **Learning from Three Case Studies**
  - **Lessons learned from 9/11**
  - **A best case example: Chicago**
  - **Indirect economic costs: Closing Pennsylvania Avenue**
- **Key Planning Considerations for High-Rise Buildings**
- **Potential Roles for Government**
- **Recommendations for Los Angeles**

RAND

We now turn to key considerations for building security.



To help building owners and security managers prioritize building safety resources, threats to Los Angeles high-rise buildings might usefully be put into three categories: highly unlikely and, for the most part, not preventable; more likely and preventable; and unlikely but possibly preventable. This categorization allows building owners and managers to funnel resources into activities and assets that will most likely be able to prevent an attack.

To define and categorize a threat, it is useful to take a two-pronged approach. First, a building's vulnerabilities should be uncovered. Second, the consequences of an attack need to be determined. Both of these aspects of threat determination will be discussed later when the *Risk Reduction Matrix* is explained.

The following are some examples of the types of attacks that fall into each of the above categories:

Horrific attacks such as that of September 11, 2001, are unlikely to be preventable by the local population and property owners. The country's national security and law enforcement agencies have the best ability to predict, prevent, and deter such events. However, these types of attacks are also highly unlikely. We would expect them to be attempted only by well-financed and equipped international terrorist organizations intent on destroying targets that

would have an impact on the national psyche or economy. The Los Angeles Police Department has already conducted its own target identification process based on national criteria for assessing the likelihood of a threat.[1]

Car and truck bombs, biological and chemical weapons attacks, and large fires are examples of the types of threats that might be preventable if enough resources are committed to deterrence technology and prevention intelligence.

---

[1] Interview with Sgt. John Sullivan, January 30, 2002.

Determining Threats and Vulnerabilities (continued)

- **General motivations for attack**
  - **Historically, there are four main motivations for terrorist acts**
    - **Symbolic attack**
    - **Intent to inflict mass casualties**
    - **Intent to disrupt infrastructure**
    - **Attempt to seize hostages**
  - **The 9/11 attack introduced the motivation to inflict economic damage**
    - **Economic consequences of 9/11 were clearly negative**
    - **Osama bin Laden has called for more attacks that create economic damage**

RAND

While it may never be known with certainty whether Los Angeles buildings are targets, educated assessments can still be made. Typically, history provides a useful guide. Historically, there have been four main motivations for terrorism: attacks on symbolic targets, the intent to cause mass casualties, acts of sabotage intended intended to cause disruption of infrastructure, and attempts to seize hostages. The events on September 11 certainly were symbolic acts and apparently were intended to cause mass casualties and infrastructure disruption.

If the state of knowledge today was precisely as it had been on September 10, then one might conclude that Los Angeles buildings would either not appear on a terrorist's target list or be far down on that list; however, the state of knowledge has changed. One of the lessons learned from September 11 by those who seek to attack American interests is the degree by which the American economy can be damaged by successfully attacking the factors of production and the inputs of the economy (namely, buildings and the people who work in them) and the harm that destruction imposes on Americans generally. Thus, while causing economic damage likely was not one of the motivations of the September 11 attacks, it was one of the outcomes, and it may be an outcome that others will attempt to replicate. Evidence of this new motivation for terrorist

activity appeared in one of the videos Osama bin Laden filmed after September 11 in which he called for followers to attack the American economy.[2] With economic damage evolving as a new motivation for terrorist activity, the possibility that Los Angeles buildings are targets has increased somewhat.

---

[2]Helen Kennedy, "Osama: Hit U.S. Economy," *Daily News* (New York), December 28, 2001, p. 9.

Determining Threats and Vulnerabilities (continued)

- **Intelligence and communication issues**
  - **Building managers must actively seek and share information with other building managers, law enforcement and intelligence agencies**
  - **Even with cooperation, threats may not be revealed**
    - **Intelligence regarding a threat might not exist**
    - **Intelligence regarding a threat might not be disclosed**
  - **Each building manager plays a primary role in determining the threats**
    - **Building owners should answer the question: Why would my building be a target?**

RAND

Determining the threat to Los Angeles high-rise buildings is not the exclusive responsibility of either law enforcement or intelligence agencies. Building owners and security managers must actively investigate their own vulnerabilities and their own potential attackers. When useful information is uncovered, it should be shared with law enforcement and similarly situated building owners as expeditiously as possible. Pooled information is one key to establishing patterns of behavior and trends that might provide early warning of an attack.

It is important to realize that threats perceived by some may not be revealed, for several reasons. First, pooled information may not in fact lead immediately to discernable patterns of behavior or other noticeable trends. This possibility should not decrease information sharing, however. Sometimes indicators can emerge relatively quickly after a seemingly long period of apparent irrelevance.

Second, given the sensitive nature of some law enforcement and intelligence activities and sources, some threats may not be revealed publicly. This may be because sources and methods need to be protected, to avoid panic or fear, or because of concern over loss of vigilance if building occupants must respond to too many "false alarms." Certainly, vague bomb threats have become common enough to warrant concern that a valid threat might not be taken seriously enough.

This is not to say, however, that specific, credible threat information will not be shared in a timely manner to those directly affected by the threat in Los Angeles.[3] Working together, building security, law enforcement, and intelligence agencies can produce responses to a threat that increase the chances that lives will be protected without undue risk.

Accepting the possibility that Los Angeles buildings could be terrorist targets, it does not follow that every building is an equally attractive target. To begin assessing the attractiveness of any building as a potential target, one might ask the question, "Why would this building be a target?" The answer would largely be based upon two variables: the vulnerabilities of a target and the potential consequences of a successful attack on the target. Holding one variable constant, as the other variable increases, the attractiveness of the target increases. A later chart contains a Risk Reduction Matrix that captures these concepts.[4]

---

[3]Author interview with Sid Heal, head of Los Angeles County Special Weapons and Tactics, February 2002.

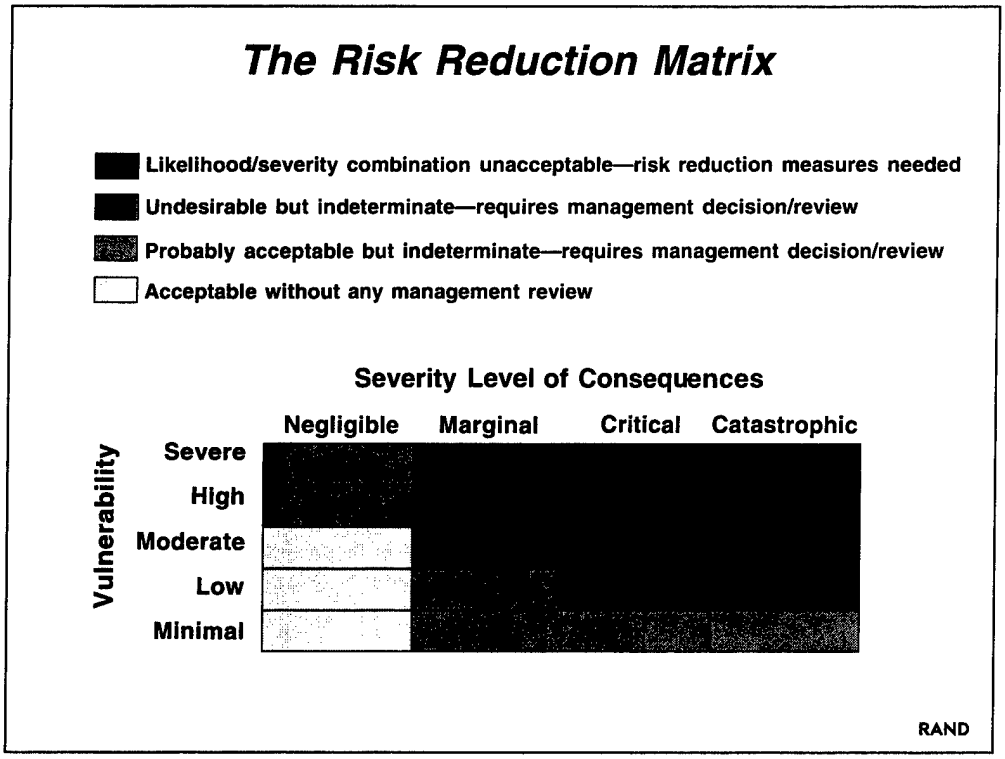
[4]Adapted from *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, Washington, D.C.: GAO/NSIAD-98-74, April 1998.

Determining Threats and Vulnerabilities (continued)

- **The Risk Reduction Matrix**
  - **A tool for assessing building-specific threats**
  - **Aids in determining whether a building needs to add security measures**
  - **Determinations based on a building's vulnerabilities to and the consequences of an attack**

RAND

The Risk Reduction Matrix, which appears on the next chart, is a tool that a building owner and manager can use for assessing threats and determining whether increased security measures are warranted. Such determinations are based on a building's vulnerabilities to a hypothesized threat and the consequences that would result from that threat coming to fruition.

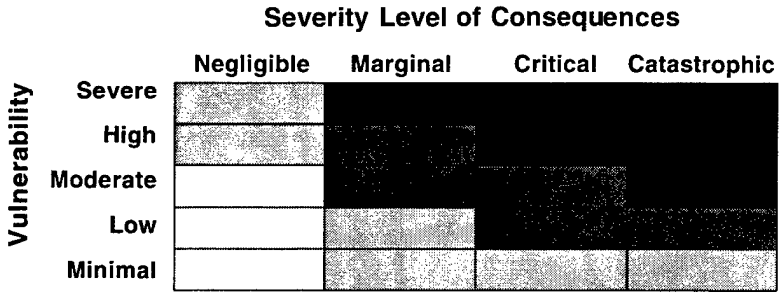


Vulnerability is a rather straightforward concept and is based mostly on the physical accessibility of the building. Consequences flow across multiple categories, and when considering buildings as targets, useful categories of consequences include casualties, economic damage, and psychological damage.

As can be seen, the further northeast a building's self-determined placement in the matrix, the more attractive the target and the greater the need to implement risk reduction (security) measures. Also clear is the general inverse relationship between vulnerabilities and consequences. Because of this relationship, those buildings for which the consequences of a successful attack would be lower have a lesser need to reduce their vulnerabilities. Similarly, those buildings for which the consequences of a successful attack would be high have a greater need to reduce their vulnerabilities.

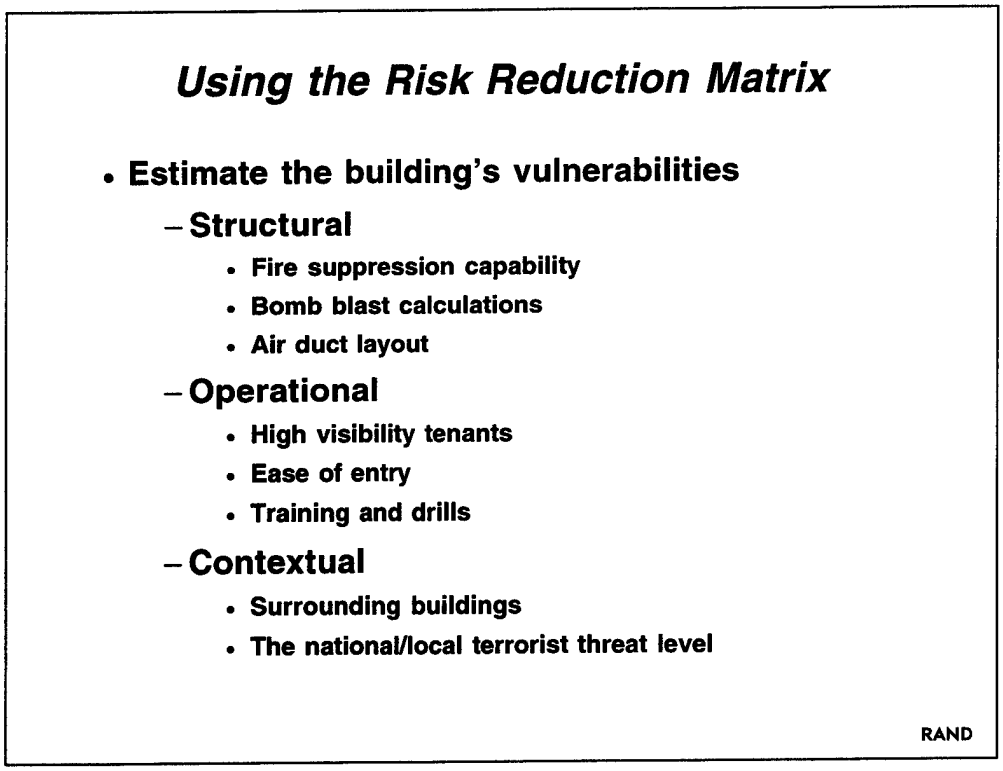
The Risk Reduction Matrix

- **Helps determine which building-specific threats require risk reduction measures**
- **Security measures can push the threat southwest**
  - **Reducing vulnerabilities moves the threat south**
  - **Reducing consequences moves the threat west**



RAND

Placing building-specific threats on the matrix illustrates to building owners and managers those threats in need of risk reduction measures. Reducing the risk can be accomplished through security measures that either reduce the building's vulnerability to the threat, thus moving it further south in the matrix, or reduce the consequences of the threat, thus moving it further west.



Those who make security decisions can use the matrix to gain a general idea about whether they need to implement more or different security measures. To do so, they must estimate their building's placement in the matrix by considering their building's vulnerabilities and the consequences that could flow from a successful attack.

There are several different categories of vulnerabilities that should be considered when assessing the overall risk to the building. Separating a comprehensive risk assessment into these categories will help building owners determine the greatest vulnerabilities, help focus security and communication efforts in these areas, and establish protocols regarding follow-on assessments. These categories will also facilitate communication among building owners, law enforcement, and intelligence agencies. For instance, understanding that a building's greatest vulnerability is that a tenant might be targeted for an attack, the building, its tenant, intelligence, and law enforcement officials can work together to ensure that all relevant information regarding would-be attackers on this tenant is shared.

An estimation of a building's vulnerabilities should include, but is not limited to, the following considerations:

Structural vulnerabilities: Structural vulnerabilities include anything intrinsic to the building that could be exploited by a potential terrorist to produce damage to the building and/or its occupants. As shown on the chart, these considerations include the limitations of the fire suppression capabilities—the sprinkler system and other hardware and practices such as fire doors and occupant movement restrictions—the vulnerability of the building's air ducts to the introduction of a hazardous substance, and the ability of the structure to withstand the blast of bombs of different sizes placed in different locations in and around the building.

Operational vulnerabilities: Operational vulnerabilities refer to dynamic building-specific characteristics (as opposed to the the static structural vulnerabilities) that can motivate a terrorist to act or can be readily exploited by an attacker. For instance, the tenancy of an icon or potentially controversial entity (such as an international economic powerhouse or an embassy), might influence a terrorist's targeting assessment, thereby increasing the likelihood of the building being vulnerable to attack. Other operational conditions, such as fire drills, emergency response training, building entry procedures and practices, can all influence a building's vulnerability to attack. The ease of entering into a building is an obvious procedural process that can be exploited by attackers if the protective procedures are not robust enough to deter them. Conversely, building entry practices could be sufficient to compel a would-be attacker to seek a different target. Training and drills can similarly dissuade an attacker eager to produce the highest amount of damage. If it is known that a particular building has better evacuation measures in place than other, similar buildings in an area, this building could be seen as a relatively less viable target of attack.

Contextual vulnerabilities: A building's proximity to other likely targets and the overall likelihood of an attack as determined by the Office of Homeland Security or its local correlate could influence a building's vulnerability to attack. If a building is close to a relatively more likely target, the building owner should consider the consequences of an attack on that other building or within the area.

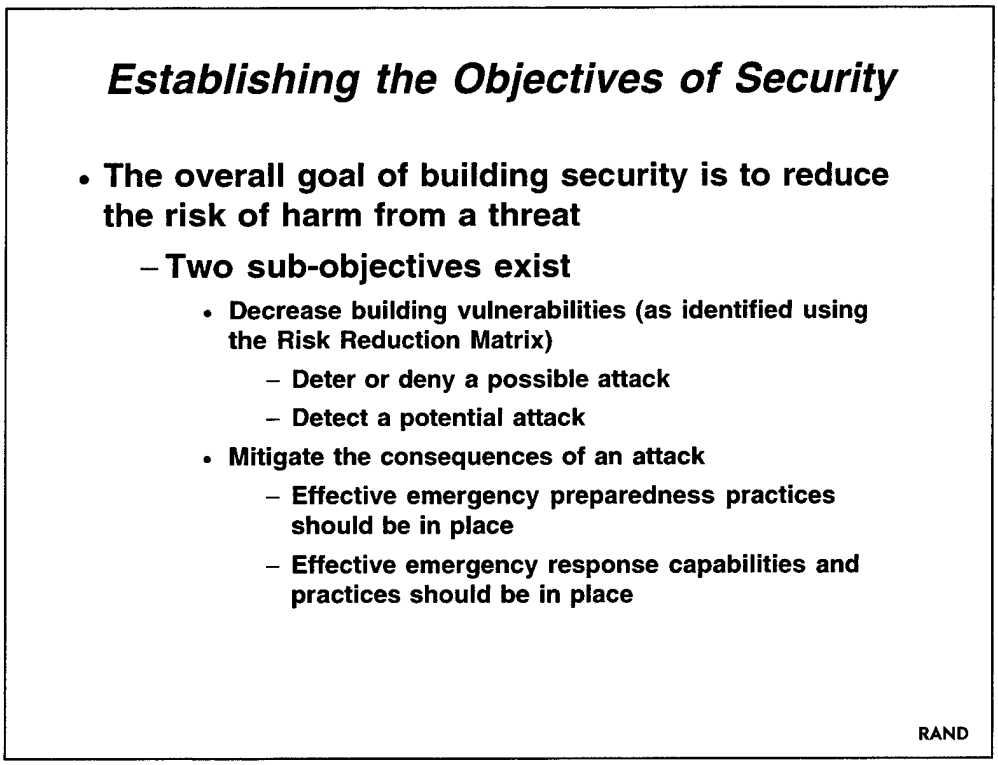
Using the Risk Reduction Matrix (continued)

- **Assess potential consequences**
  - **Building-specific consequences**
    - **Should be determined based on losses from the damage of a particular building, including:**
      - **Casualties**
      - **Economic damage**
  - **General consequences from an attack on any L.A. office building**
    - **Should be done in conjunction with law enforcement, emergency responders, and intelligence agencies**
      - **General fear**
      - **Sense of vulnerability**

RAND

Consequences have two components: The first is building specific, and the second is more general. The building-specific consequences (casualties, resultant economic damage, and the symbolic nature of the building) depend largely on the stature of the building and the number and type of tenants. The more general consequences are those that would result from a successful attack on any building. They include the psychological effects of increased fear and a greater sense of vulnerability. These too have downstream economic consequences, such as diminished productivity of workers, loss of downtown business, and longer-term loss of downtown tenants.

Once a decisionmaker understands the building's vulnerabilities and the consequences in the event of a successful attack, decisions can be made as to whether security measures should be modified.



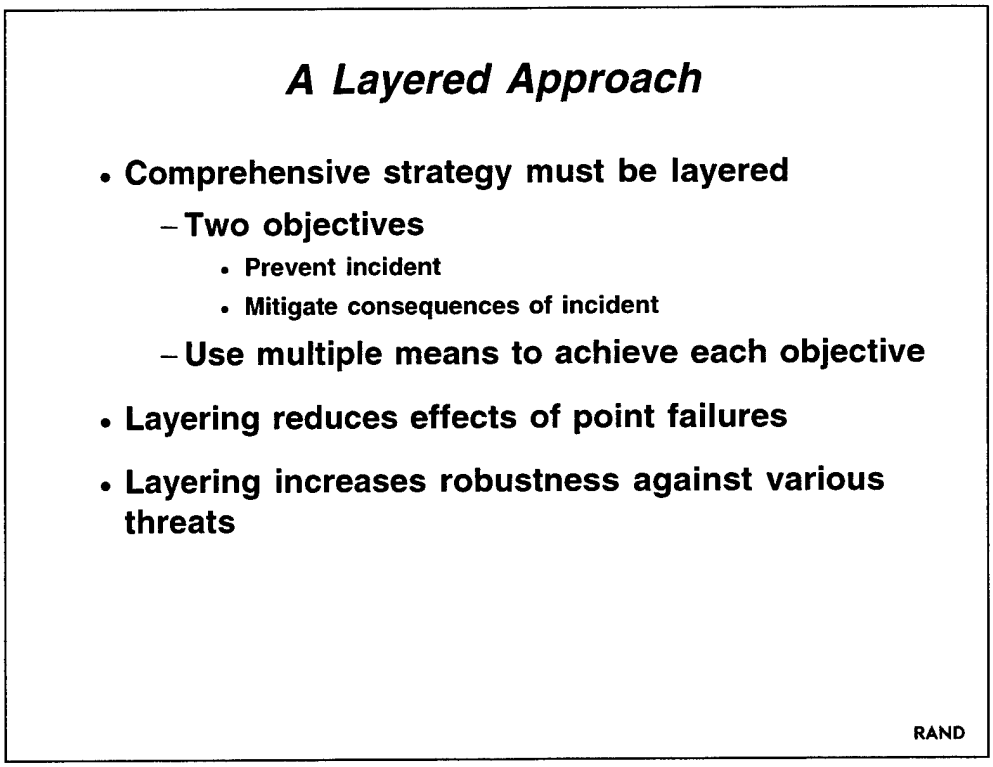
The overall goal of security measures is to reduce risk, which is composed of two components. One is to decrease vulnerabilities with the aim of preventing an attack. On the Risk Reduction Matrix, this would shift the target further south. The other is to mitigate the consequences of a successful attack. On the Risk Reduction Matrix, this would shift the target further west.

Prevention has many layers, the bulk of which are decided at the top levels of the federal and state government and are beyond the control of those who make building security decisions. Such layers include customs policies, intelligence funding and methods policies, and law enforcement policies. The prevention decisions within the control of building owners and managers center on "hardening the target," which can accomplish (1) deterrence and (2) detection and denial.

Deterrence is achieved through the visibility of effective preventative measures. The effect of deterrence is in convincing those considering an attack that they should not do so because the chance of success is too low. In effect, it stops the attack before it starts. The September 11 attacks may be instructive here. One of the stunning aspects of the attacks was that the attackers apparently were convinced they would succeed. One can speculate that the time, money, and human capital invested to undertake the attack may have been invested because of a perceived lack of effective security.

Detection and denial are achieved through effective preventative measures, regardless of whether they are visible. For example, security measures such as motion sensors and hidden cameras will serve no deterrent effect but will aid the visible security measures, such as guards and access controls, in detecting an attack and denying its success. While the effect of deterrence is to stop an attack before it starts, the effect of detection and denial is to stop an attack that has already commenced.

The other objective of security measures is to reduce the risk through response. Response is aimed at mitigating the consequences of a successful attack. Response measures can be extremely effective in saving lives and minimizing other consequences. As later charts note, 99 percent of those below the crash floors in the World Trade Center (WTC) survived largely due to WTC response measures.



A comprehensive security strategy must include multiple layers. Measures should be aimed at both preventing an attack from succeeding and responding to mitigate the consequences in the event one does. In addition, within the sub-objectives of prevention and response, multiple measures should be used to achieve each.

There are two primary rationales behind the need for multiple layers. First, redundancy reduces the likelihood that an individual point failure will result in catastrophic consequences. If one layer is breached, other layers may prevent the attack, and if the attack succeeds, still other layers can reduce the consequences of the attack. Second, redundancy increases a building's robustness to various threats. Because the particular threats a building may face are unknown and constantly evolving, security must be broad enough to prevent or respond to these unforeseen and unknown threats.

Understanding Existing Security Practices and Technologies

- **Prevention measures**
  - **Exterior**
    - **Physical control**
    - **Perimeter awareness**
  - **Access control**
  - **Subterranean parking control**
  - **Internal control and awareness**
  - **Mail and deliveries**
  - **Tenant participation**
- **Response measures**
  - **Firmly established event-specific protocols**
  - **Tenant awareness of protocols**
  - **Ability to notify quickly—a public address system**
  - **Testing**
- **The technology market**

RAND

A selective survey of Los Angeles high-rise office buildings reveals that prevention and response measures are spread across several areas. Prevention measures focus on the exterior (including physical control beyond the building and perimeter awareness), access control, subterranean parking control, internal control and awareness, handling of mail and deliveries, and tenant participation. Response measures are concerned with developing firmly established event-specific protocols, ensuring tenants are aware of those protocols, and testing the response of tenants and security through drills. The following charts describe the measures building security personnel are using and the degree to which they are using them.

Understanding Existing Security Practices and Technologies (continued)

- **Prevention measures**
  - **Exterior**
    - **Physical control**
      - **Bollards-fixed**
      - **T-rails (Jersey barriers)**
    - **Perimeter awareness**
      - **Cameras**
      - **Guards**

RAND

The exterior security measures include physical control and perimeter awareness. Physical control measures are those that extend security's physical control beyond the building itself. These have been limited to the use of fixed bollards (metal posts that delimit an area) and T-rails (sometimes called Jersey barriers, which are concrete barriers typically about 3 feet high and 15 feet long). Currently, only a few buildings employ such measures. Those that do have them use them almost exclusively to shield a primary entrance.

Perimeter awareness is more common, although still not as visibly prevalent as one might expect. Perimeter awareness consists of exterior cameras and guards who are typically limited to a periodic patrol. In general, camera coverage is quite variable across buildings. It appears to be concentrated primarily on points of ingress and egress, as one might expect, with less attention given to other potential vulnerabilities such as contiguous streets. Additionally, new camera technology seems to have bypassed some of the buildings in Los Angeles, and owners are likely to be reviewing and upgrading their equipment in the future. Some visible exterior cameras are obviously obsolete and in at least one instance, obviously not working. It is unclear whether a large visible camera that is not working is intended to "lull" a perpetrator into believing a

property is unprotected when in fact modern, invisible equipment has been installed elsewhere, or whether a nonworking camera represents a true security lapse. Because cameras have some potential deterrence effect and substantial forensic value, all owners and security managers should thoroughly assess their camera systems.

Understanding Existing Security Practices and Technologies (continued)

- **Prevention measures (continued)**
  - **Access control**
    - **Limiting points of entry**
    - **Access cards/turnstiles**
    - **Visitor control**
  - **Subterranean parking control**
    - **Automated access control**
    - **Supplemented with guards**
    - **Valet only**
    - **Visitor control**
    - **Vehicle search**

RAND

Access control is the most extensively used security measure. All buildings have some form of access control measures, and most have either upgraded their access control systems or are planning to do so. As an initial step, most buildings have limited their points of entry and exit so that all people entering the building must pass by guards. From there, the particular procedures vary among buildings. For example, in some, tenants just show their photo identification access card to a guard; some use turnstiles; and others utilize a system by which tenants swipe their identification card for entrance and exit. With this type of system, security has the capability of knowing precisely which tenants are in the building.

Most visitor control is limited to requiring a visitor to show identification and sign in, but other buildings have increased measures, including a guard verifying that the company and floor the visitor reports he is going to match each other, preauthorization for visitors, calling a tenant to announce/verify visitors. One building we visited is acquiring a system whereby tenants can register a visitor online and a visitor badge will print out. Requiring visitors to sign out is relatively rare. Thus, security often has no mechanism for knowing whether any visitors remain in the building and, if they do, who they are.

Subterranean parking control has also increased almost universally. Most buildings have stationed a guard at the lot's entrance and maintain periodic patrols. Typically, the guards ensure that tenants swipe their cards and check identification and/or record the license plate of visitors. The guards may also conduct a cursory visual search of the car, the effect of which is only to catch the obvious. More extensive measures include calling the tenants for all visitor verification, conducting random searches of tenants' cars and searching the cars of all visitors, searching all enclosed vehicles (i.e., vans), only permitting valet parking, and stopping each car before it enters the lot to ensure it is permitted to access the lot.

Understanding Existing Security Practices and Technologies (continued)

- **Prevention measures (continued)**
  - **Internal control and awareness**
    - **Elevator control**
    - **Cameras**
    - **Guards**
  - **Mail and deliveries**
    - **Screening delivery vehicles**
    - **Guards or cameras in the loading dock**
    - **X-ray mail**
    - **Tenant notification of delivery**

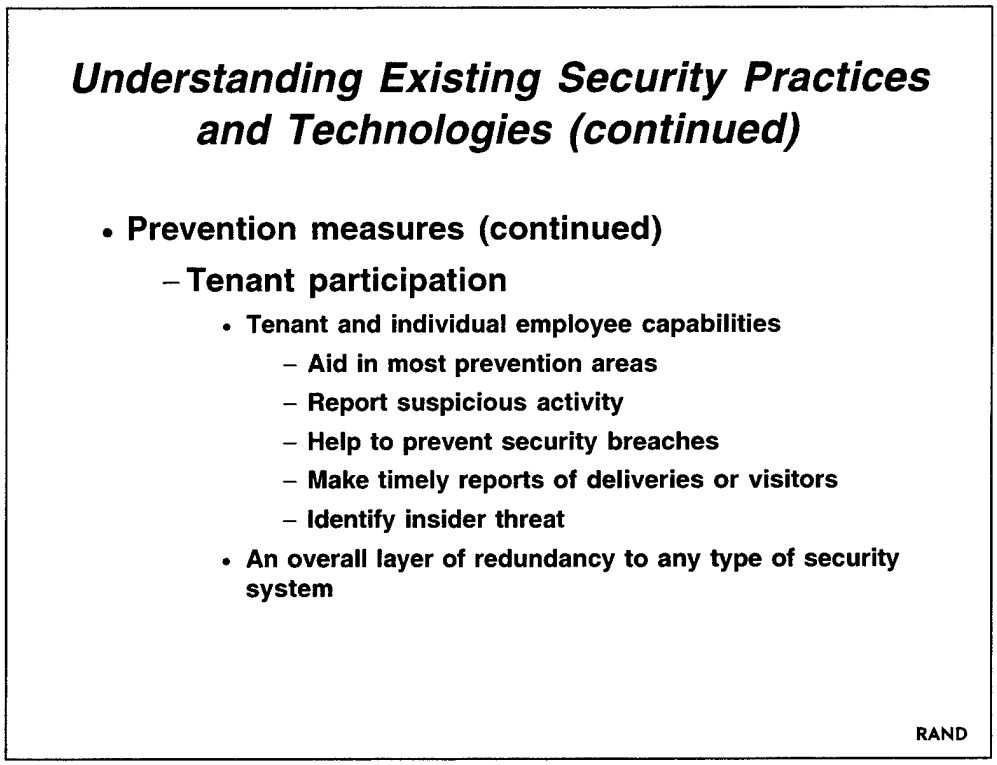
RAND

Internal control and awareness is less prevalent than access control. The prime tools are elevator control, cameras, and guards. Most buildings have some form of elevator control based on swiping an access card against a sensor in the elevator. After the swipe, the systems vary. Some allow access to any floor. Some allow access to only those floors to which the card is registered. Additionally, some systems require that only one button can be pushed for each card swipe, while others permit multiple buttons to be pushed after a single swipe. Those that are less restrictive allow for the possibility that people can gain access by "piggy-backing" or "tailgating" on another's card swipe.

Other than elevator control, internal control and awareness are relatively minimal. Cameras are used, although not extensively. Guards patrol the building, but they cannot be everywhere. Building staff have been trained to be alert to unusual circumstances or people, but most building occupants rarely consider a practice of enhanced awareness as part of staff responsibility.

Security measures regarding mail and deliveries are also relatively minimal, concentrating almost exclusively on delivery vehicles or the loading dock. Most delivery vehicles are searched, and most loading docks have either a guard or a camera. Some buildings have a guard that signs in packages or notifies tenants when a package arrives.

One building x-rays its mail, but that building also allows hand carried packages to be taken to tenants without being x-rayed. Overall, building managers are uncertain about the appropriate security for movement of goods into the building.



Tenant participation is an underutilized but essential layer of prevention measures. Tenant participation can be considered a last line of defense in that if all other layers (exterior awareness, access control, internal awareness) are breached, an aware tenant can aid in foiling an attack. A useful example is the case of Richard Reid, more commonly know as "the shoe bomber." Reid breached several layers of airport security, including preliminary questioning by the ticket agent, screening at the security checkpoint, and more intensive questioning when he alerted suspicion at the gate. None of these layers was successful in preventing the attack. Reid's intended attack was thwarted by an alert flight attendant and some alert and active passengers, essentially the last line in a layered system of security.

Likewise, the tenants of buildings can and should be a security layer. Specifically, tenants can aid in the following areas: perimeter awareness by notifying security of suspicious cars or vans, access control and internal control by ensuring that nobody "piggy backs" their card swipes at an entrance point or in an elevator, and internal awareness by notifying security of suspicious people or packages inside the building. Tenants can also assist security by timely reporting of anticipated deliveries or visitors. Finally, tenants can help ward off the threats posed by insiders by heeding the advice of security personnel and experts regarding the importance of conducting, and how to conduct, background checks on prospective employees.

Understanding Existing Security Practices and Technologies (continued)

- **Response measures**
  - **Firmly established event-specific protocols**
    - **Four main responses**
      - **Full building evacuation**
      - **Fire response**
      - **Tenants do nothing while security investigates the incident**
      - **Individual floor lockdown**
  - **Tenant awareness of protocols**
  - **Ability to notify quickly—a public address system**
  - **Testing**

RAND

Response measures focus on mitigating the consequences of an event by following firmly established protocols. Currently, buildings have four main response protocols: a full building evacuation, a fire-type response that calls for evacuating and relocating specific floors, a security investigation only, and an individual floor lockdown. Except for the final measure, which is followed in most buildings in response to the suspicion of a chemical or biological substance, several building managers are not yet certain which responses should be utilized for which events.

For a response measure to be effective, three things are required. First, the tenants must be aware of the measures. Tenants have to know precisely what they are expected to do. The mechanisms for informing tenants of procedures varies among buildings. At one end of the spectrum is an informal notification process whereby security informs tenants' assistants. At the other end of the spectrum is a formal process whereby security and tenant representatives hold frequent, regular meetings to discuss issues such as new or altered protocols.

Second, there must be an ability to notify tenants that a response protocol is being used when an event has occurred. In many buildings, this is done through a public address system that is capable of being used when primary power is not available. This

process can be modular and computer driven or handled by human beings. In some cases, depending upon the threat, phone calls may be used.

Third, tenants and security must be able to perform the response measures. To ensure this, drills must be held. However, in most buildings drilling occurs only to the minimum extent required by law, and there are indications that some tenants do not participate in even these drills. Additionally, in many buildings the drills are performed in conditions that are relatively artificial, such as conducting a full evacuation drill but only doing so a few floors at a time.

Understanding Existing Security Practices and Technologies (continued)

- **The technology market**
  - **Prevention**
    - **Upgrades**
    - **Weight determination**
    - **Biometrics**
    - **Chem/Bio detectors**
    - **Visitor tracking**
  - **Response**
    - **Evacuation Slides**
- **More measures may not be needed**

RAND

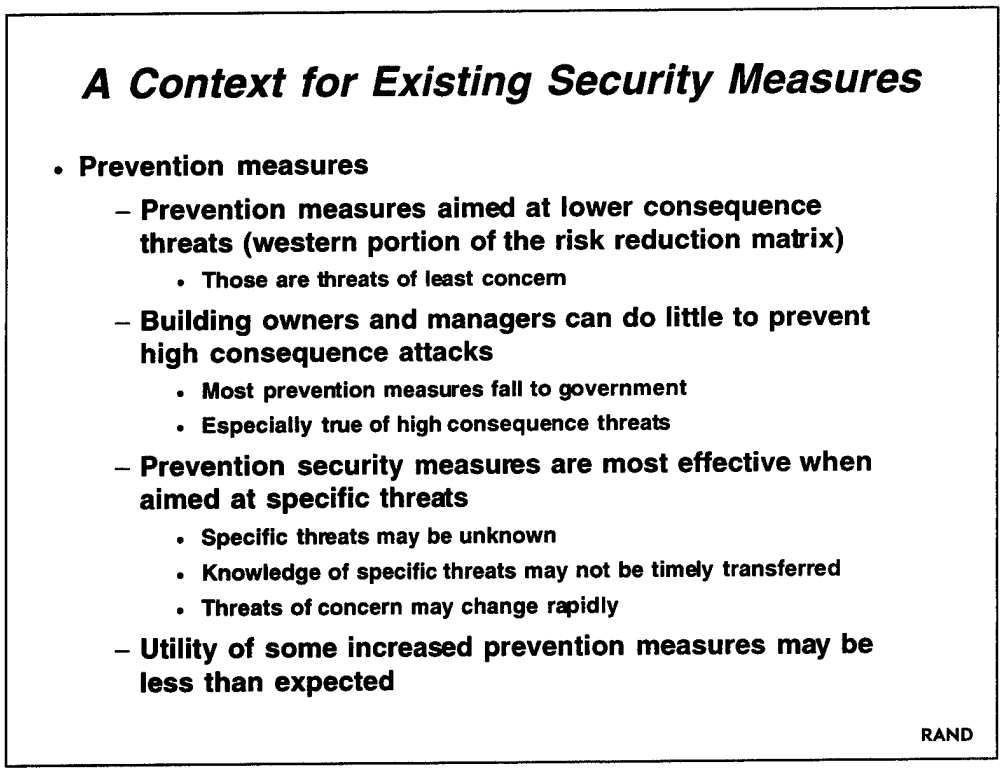
As in many areas, technology in building security is constantly improving and offering the ability to do more. At an initial level, technology allows those systems currently in use to be upgraded or otherwise made better. Cameras are smaller, lighter, have better pictures, and can be set to automatically pan and scan. Video from any closed circuit television camera can be set to be viewed on any computer on or off site. All video can be stored digitally on hard drives and set to record only when there is movement or somebody or something in view. Software can be used with cameras so that they can detect and sound an alarm in response to certain movements (e.g., those that would indicate a car thief in a parking lot).

Systems utilizing card swipes can be integrated into every door and elevator in the building, allowing access only to those floors and offices for which the card holder is authorized. Bollards can be made to be retractable and used for a number of purposes, such as making access to a subterranean garage more difficult for those who are unauthorized. The ease and speed with which video and other information can be transmitted allow for security systems to be administered completely off site or otherwise outsourced.

Aside from the general upgrades of current systems, technology also offers items fundamentally distinct from anything that has been in

use previously. The weight of a vehicle can be assessed from afar to aid in determining whether it carries heavy explosives. Biometrics can be used for access and internal control. Chemical and biological sensors can detect the presence of dangerous pathogens or toxic agents. Visitors can be assigned "smart cards" that will track their whereabouts throughout a building. Undoubtedly, other advanced technological security currently exists or will soon be developed.

The question is not whether we can do more to harden a building, for we can always do more to harden any target. The question is whether we should do more to harden a target. Some sense of context is required. The types of security options available above may be too costly and yield too little benefit given the nature of the threats with which building security is concerned.



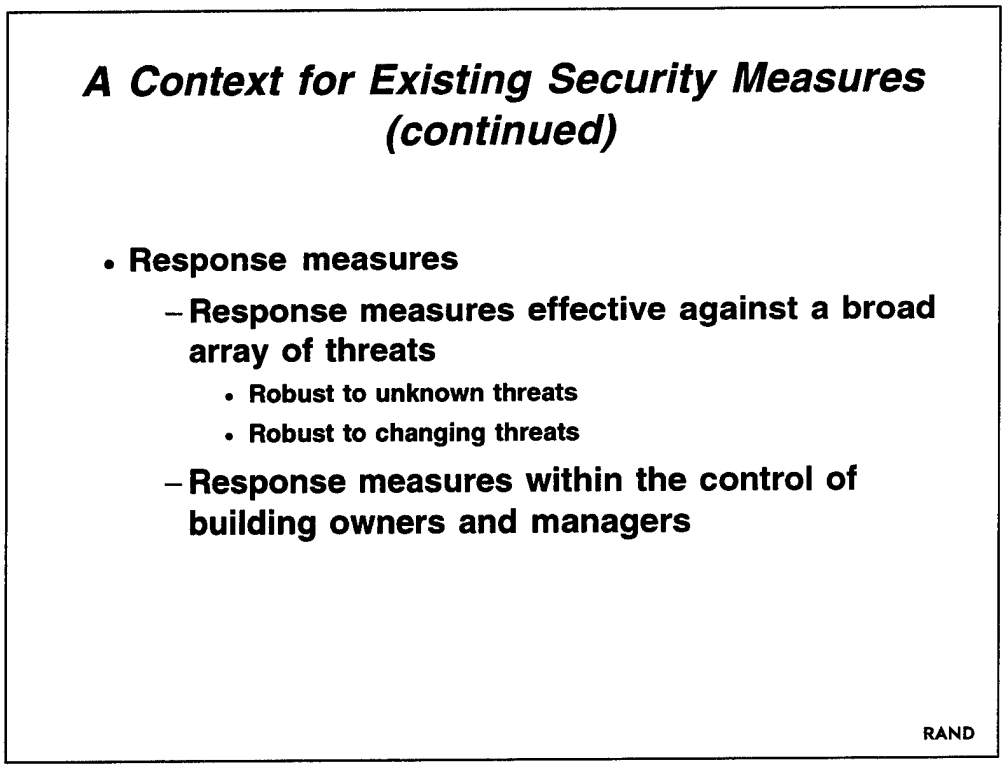
The prevention measures implemented in the wake of 9/11 have centered on access control and subterranean parking control, and, to a lesser extent, internal and exterior awareness. These measures have two goals: (1) keeping out of the building those people who present themselves to enter and do not belong or may inflict harm, and (2) gaining an awareness of those people, either inside or outside the building, who arouse suspicion. The threats that these measures would prevent are lower consequence threats. First, those seeking to inflict critical or catastrophic harm are unlikely to present themselves to enter. Second, those who gain access are unlikely to do so with implements or equipment capable of inflicting critical or catastrophic harm.

Prevention measures aimed at stopping high-consequence attacks are mostly under the control of government and beyond the capabilities of building owners and managers. Such measures include combat air patrol; cultivating, gathering, processing, analyzing, and disseminating intelligence that assists in identifying individuals or groups who are planning such attacks; decisions about who may enter and remain in the country; etc.

The prevention measures within the control of building owners and managers are most effective when tailored to prevent specific threats. If security personnel have information about a potential threat, they

can implement measures aimed at preventing that threat. For example, if there is information that a truck filled with explosives will be used to carry out an attack, it is relatively unproblematic to implement security measures that would prevent such an attack. Equipment could be purchased or procedures could be implemented to prevent most specific threats, but if the threat of concern changes, it may be useless against the new threat. For example, at great expense, machines could be obtained so that all mail could be irradiated, thus killing anthrax, a threat that has received much public attention. Such a measure, however, would do little to prevent a threat of chemical weapons release.

Without specific knowledge regarding what to prevent, effective security measures are difficult to implement. They require screening for *anything* potentially dangerous. That would be an unrealistic charge for security officials and building owners and managers.



In contrast to prevention measures, which are most effective when tailored to prevent a specific threat, response measures can be effective to mitigate the consequences of a broad array of threats. Prevention measures are meant to stop an attack, but the potential attacks upon a building are limitless. Response measures are meant to mitigate effects, and effects are finite.

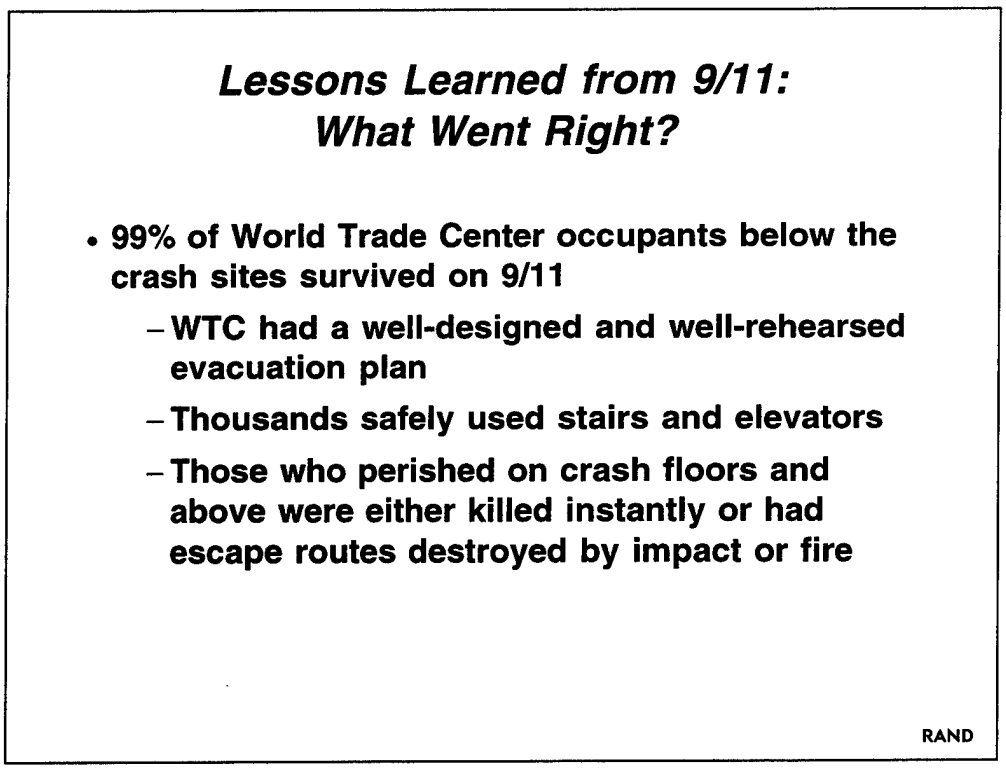
The basic goal of response measures is to limit the damage inflicted by a successful attacks. The basic means is by quickly removing people from the zone of danger created by the attack and minimizing that zone of danger. The goal and means change little, if at all, for most conventional explosive and incendiary attacks. It does not matter whether a car bomb, plane, or other conventional explosion causes structural damage to the building. The response to such structural damage is expected to be the same. The response to certain weapons of mass destruction attacks may vary, particularly if there is a need to control the movement of people so that the threat of spreading a contagious disease can be assessed.

Briefing Outline

- Introduction and Summary Observations
- Key Considerations for Building Security
  - Defining the threats and vulnerabilities
  - Establishing the objectives of security
  - Understanding existing security practices and technologies
  - A context for existing security measures
- √ Learning from Three Case Studies
  - Lessons learned from 9/11
  - A best case example: Chicago
  - Indirect economic costs: closing Pennsylvania Avenue
- Key Planning Considerations for High-Rise Buildings
- Potential Roles for Government
- Recommendations for Los Angeles

RAND

We now turn to lessons derived from three case studies.



Municipal High-Rise Policy Changes after September 11

Given the enormity of the September 11 disaster, it is only natural that we ask, "What went wrong?" The question expresses the forward-looking desire to avoid such calamities in the future. A less frequently asked question, though one of perhaps equally great import and vision, is "What went right?" on September 11. What, despite the relative unpredictability of what specifically happened, was well planned for? Indeed, with regard to high-rise building preparedness, this latter question appears to be the more relevant of the two.

Validation of Conventional Wisdom and Planning

Although many studies can be expected in the future, *USA TODAY* performed a remarkable analysis of the attack on the twin towers of the World Trade Center. It focuses on who died, who lived, and whether their location in the buildings was a factor in their fates. The results are dramatic: "In each tower, 99% of the occupants below the crash survived. At the impact area and above, survival was limited to just a handful of people in the south tower who made an amazing escape."[5]

---

[5]Dennis Cauchon, "For Many on Sept. 11, Survival Was No Accident," *USA TODAY*, December 19, 2001.

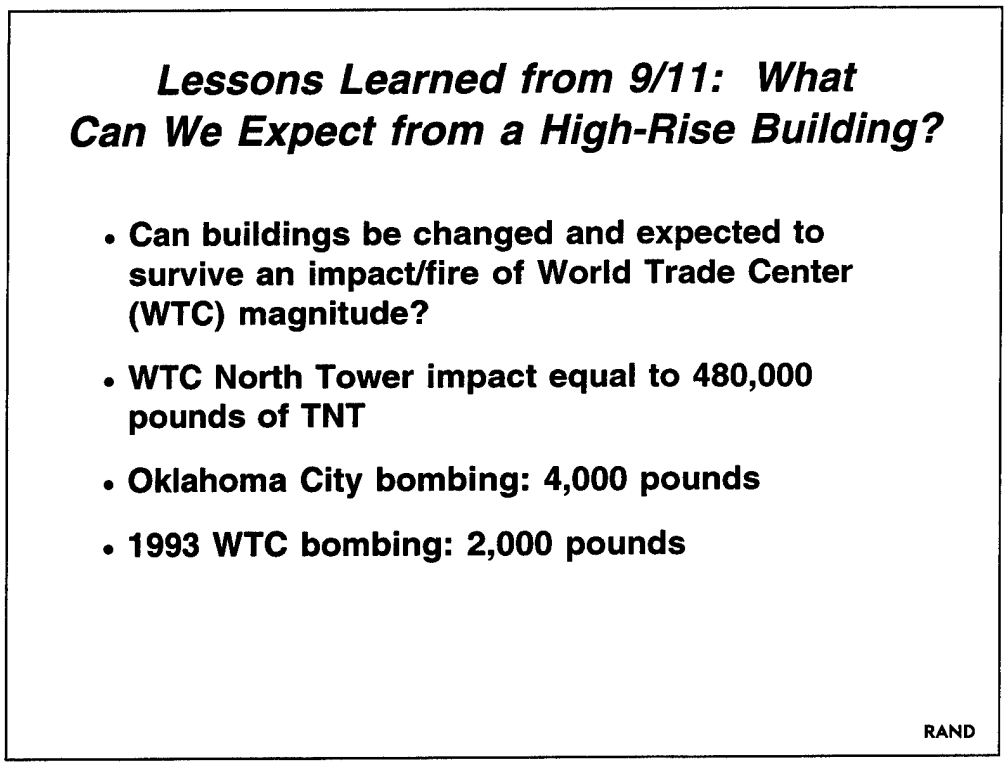
The bottom line of the analysis can be summarized in a few simple points:

- The WTC had a well-defined and well-rehearsed evacuation plan (significantly revamped since 1993) that worked well.
- Thousands of people situated below the crash sites were able to use both stairways and elevators to get out of the buildings before their ultimate collapse.[6]
- Those on the floors of and above the crash sites were either killed instantly, or were unable to escape because most of the stairways leading down were blocked.[7]

---

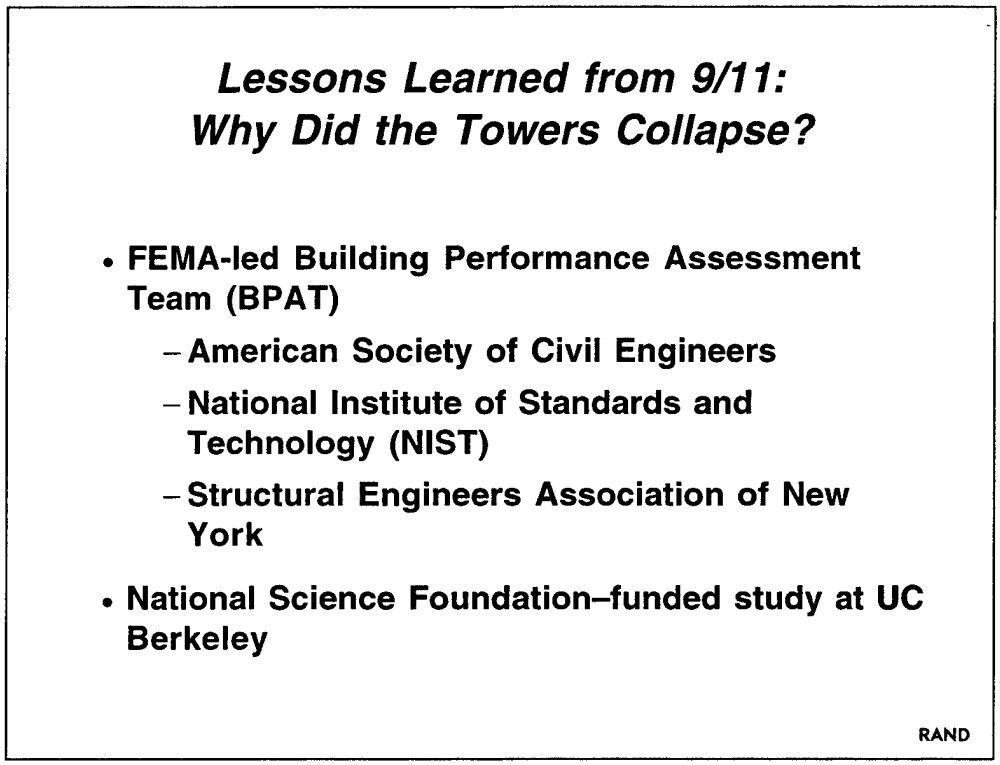
[6]A small number perished on the roof waiting for a helicopter rescue that was impossible because of smoke.

[7]Steven Ashley, "When the Twin Towers Fell," *Scientific American*, October 9, 2001.



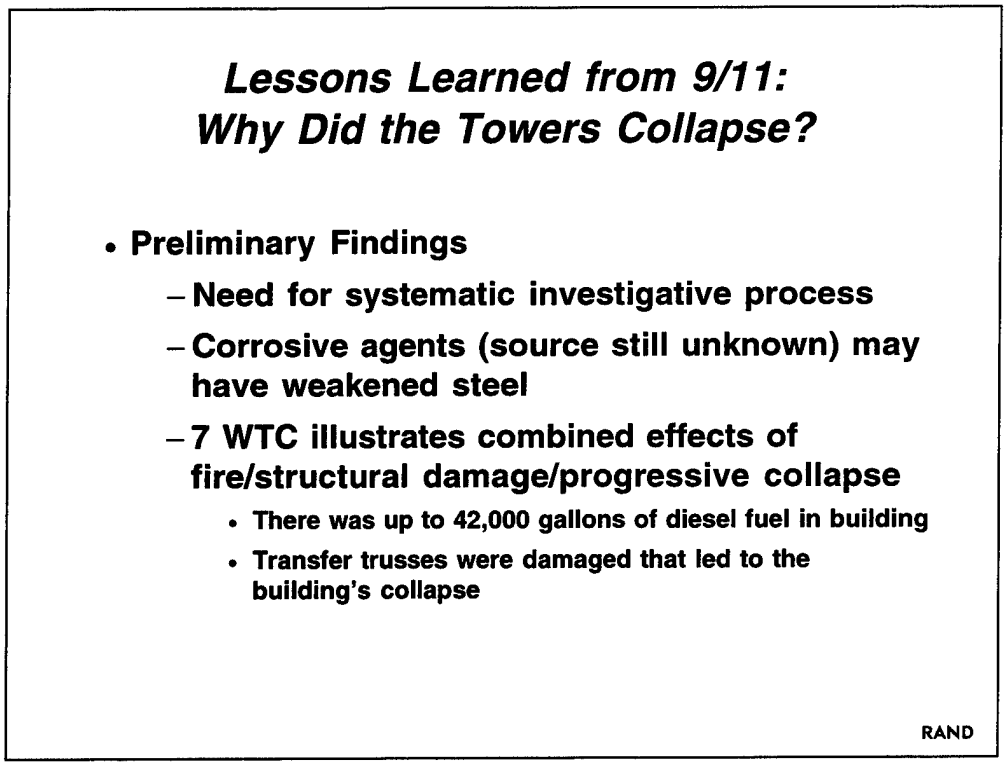
The *USA TODAY* article notes that the Boeing 767 hit the north tower with a force equal to that of about 480,000 pounds of TNT. Keeping in mind that the blast that sheared the face off of the Murrah Federal Building in Oklahoma City had a force of about 4,000 pounds of TNT (i.e., a force slightly more than eight tenths of one percent of the September 11 WTC impact), and that the 1993 WTC bombing had a force of a "mere" 2,000 pounds of TNT, one can say it is remarkable that the WTC towers remained intact as long as they did. It appears that high-rise buildings may be built or reinforced to withstand such an initial impact, but several analyses under way suggest that the heat from the blast and the resulting fire may weaken the structure so that intact lower floors cannot stand the force of the collapsing upper floors.

However, there is reason for optimism. It remains extraordinarily difficult to field and deliver a weapon—conventional or otherwise—with a 240-ton yield, especially from the ground.



A number of agencies are investigating the physical collapse of the World Trade Center towers as well as the 47-story 7 World Trade Center. The main assessment is being conducted by a Federal Emergency Management Agency (FEMA)-sponsored Building Performance Assessment Team (BPAT), which includes representatives from a number of relevant public and private-sector organizations.

Members of the BPAT provided their first report to Congress in early March (see www.house.gov/science). The full report of the BPAT is expected later in 2002.



Members of the BPAT recommended the development of a systematic investigative methodology for disasters akin to that in place for aviation disasters. The lack of such a methodology has compounded the difficulties in the current assessment.

Many questions have been raised about the combination of impact and fire that precipitated the WTC collapse. Investigators now have an additional factor to include: the presence of a corrosive material, which might have weakened the building's steel.[8]

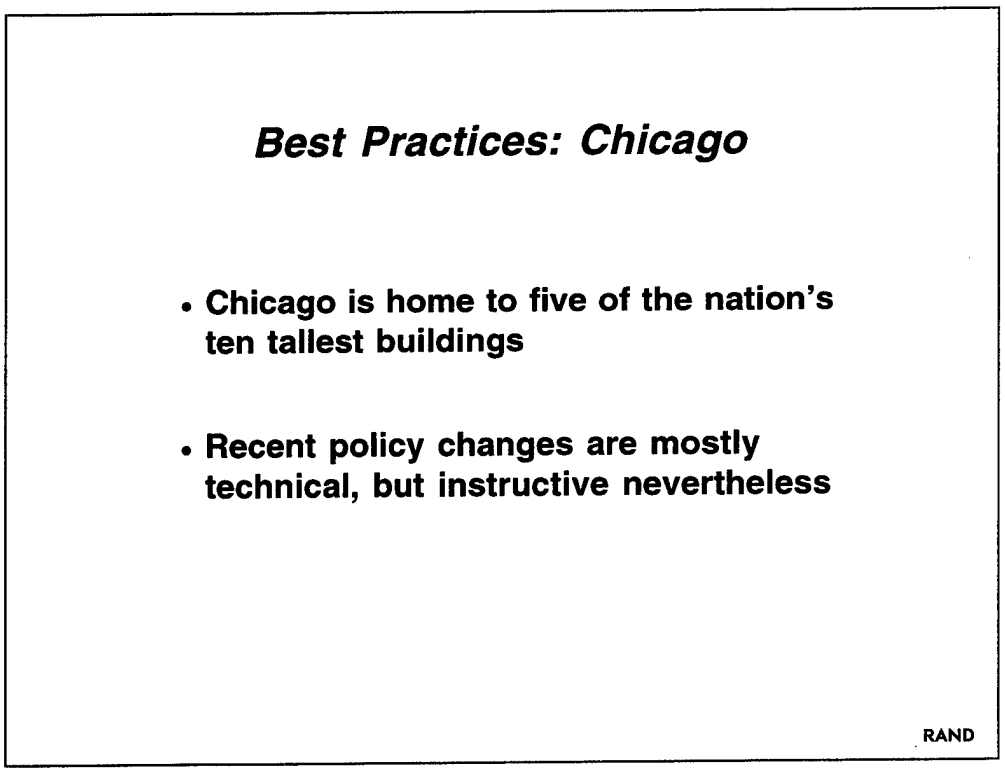
It has been determined that in 7 WTC, a seven-hour fire fed by diesel fuel stored on-site for the emergency power needs of federal and local emergency agencies (including the Secret Service and the NYC Office of Emergency Management) weakened a transfer truss, which led to the building's collapse. A similar structural failure contributed to the collapse of the Murrah Federal Building in Oklahoma City in 1995.[9]

---

[8]James Glanz and Eric Lipton, "A Search for Clues in Towers' Collapse," *The New York Times*, February 2, 2002.

[9]James Glanz and Eric Lipton, "Burning Diesel Is Cited in Fall of 3rd Tower," *The New York Times*, March 2, 2002.

As noted earlier, it also appears that the tremendous heat generated by the blast upon impact served to disable the sprinkler systems and other fire suppression measures and to melt the structure of the upper floors to the extent that their pancake-like collapse generated too much force for the intact lower floors to withstand.



In Chicago, home to five of the nation's ten tallest buildings, there have been a number of recently implemented high-rise building policy changes, most of which are in response to the events of September 11. The changes primarily concern various technical aspects of evacuation, including (1) the designation of on-site building fire safety directors, fire wardens and emergency evacuation teams; (2) the frequency of safety drills (twice annually for buildings over 780 feet tall, once yearly for buildings over 540 feet tall); (3) the distribution of emergency information to tenants; (4) emergency evacuation plan documentation; (5) special assistance for disabled building occupants; and (6) specifics about the labeling of stairwells, elevators, and areas of rescue assistance.

Best Practices: Chicago (continued)

- **Chicago High-Rise Evacuation Ordinance**
  - **Passed by City Council in October**
  - **Mandates and regulates high-rise evacuation planning and training at the building level**
  - **Requires certified fire safety directors**
  - **Details frequency of evacuation drills**

RAND

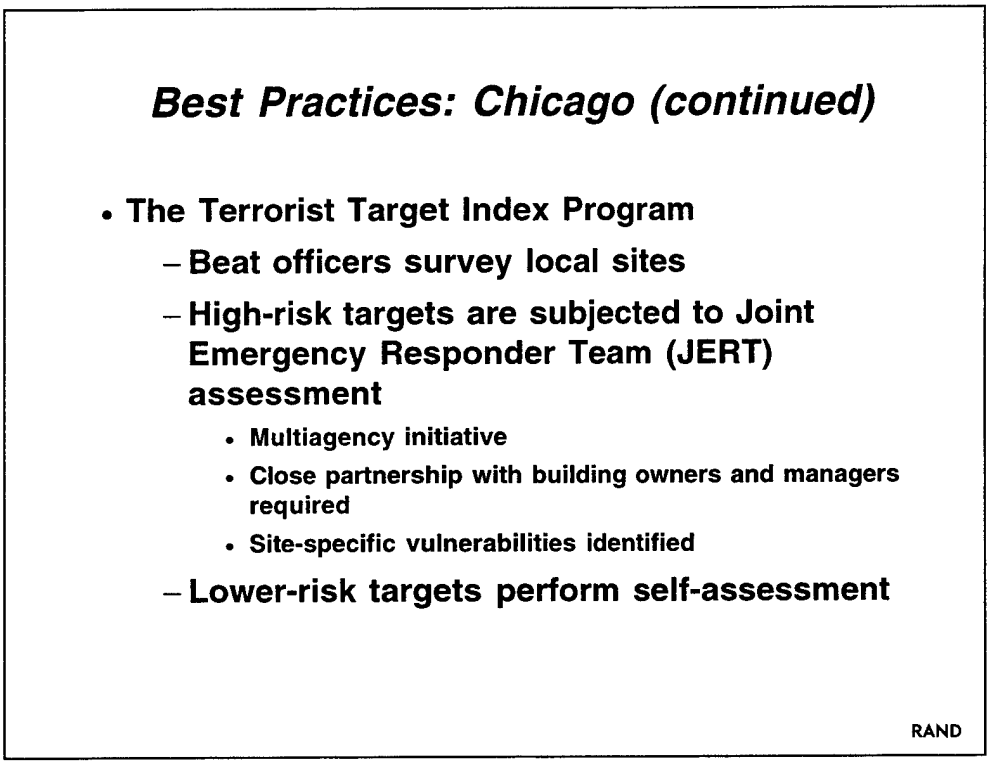
The Chicago City Council passed the Chicago High Rise Buildings–Emergency Procedure ordinance on October 31, 2001. According to the ordinance, high-rise fire safety directors (FSDs) and deputy fire safety directors (DFSDs) must obtain an Emergency Preparedness Certificate. In order to do so, FSDs and DFSDs must attend a two-hour class that covers the high-rise emergency procedures detailed in the Chicago Municipal Code (Chapter 13-78). By requiring building FSD certification, the city has made involvement in evacuation planning and training at the building level both mandatory and regulated.

Best Practices: Chicago (continued)

- **Office of Emergency Communications**
  - **Office coordinates communications for fire, police, EMS**
  - **High-rise buildings must submit on CD:**
    - **Floor plans**
    - **Evacuation routes**
    - **Contact information**
    - **Locations of those requiring special assistance**
    - **Other vital data**
  - **Data can be transmitted in real-time to on-scene responders**

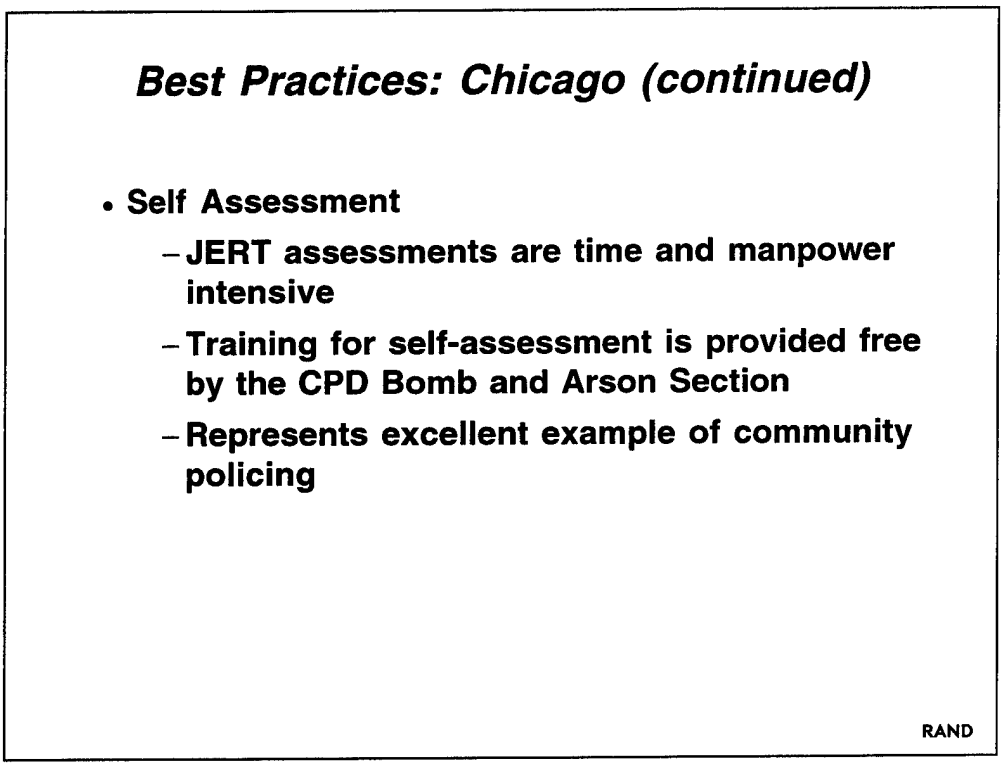
RAND

High-rise buildings must now provide the Chicago Office of Emergency Communications (OEC) with a compact disc (CD) at least every six months containing detailed floor plans, evacuation routes, text documents for each floor, contact information for the entire building, a file showing occupants needing special evacuation assistance, their specific location and the type of assistance required, and a host of other vital building data, all in standard formats. The OEC thus maintains a reasonably current, electronic "target folder" (to use the Los Angeles parlance) for each high-rise building. The usefulness of target folders is discussed further, below. The OEC is able to transmit textual data to all Chicago Police Department (CPD) squad cars. More detailed information, including the floor plans and other graphics, can be sent to police and fire mobile command units and to emergency medical services (EMS) that would be present at any large-scale disaster.

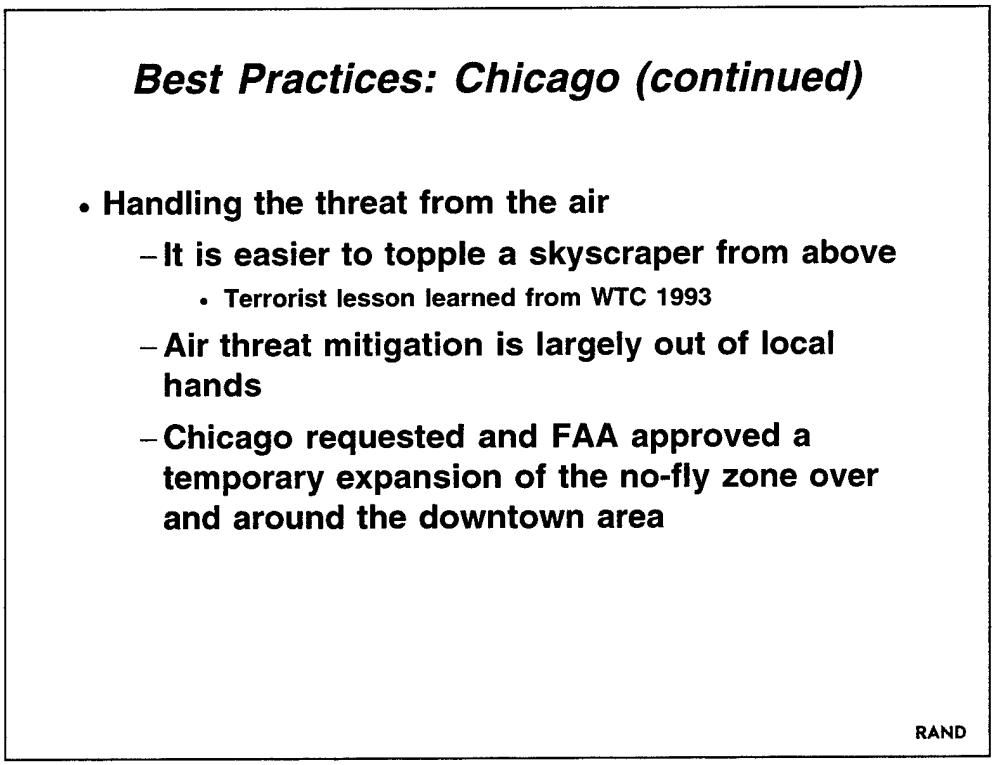


The data mentioned above are required of all high-rise buildings, regardless of the perceived or real terrorist threat to them. Beginning in 1998, the city also initiated a program for threat assessment and preparedness, the Terrorist Target Index Program. This program starts bottom-up, at the beat patrol level, with officers filing surveys of potential targets, which are classified according to perceived threat level (low, medium, or high). High-risk targets are also identified by direct request from a given location's management and from the top-down within city agencies as well. High-threat targets are subjected to a Joint Emergency Responder Team (JERT) assessment.

The JERT's members include a Chicago Police Department explosives technician, a Chicago Fire Department (CFD) hazardous materials (HAZMAT) technician, a member of the FBI's Chicago field office Terrorism Task Force, a representative of the CPD Hostage, Barricade and Terrorism Unit (HBT) and the CPD's Terrorist Target Index coordinator, who is a member of the CPD Bomb and Arson Section. The JERT Assessment has two functions. First, the JERT identifies vulnerabilities at a high-risk site to the facility and building managers and heads of security, who accompany the JERT on their walk-though survey, so that these vulnerabilities can be addressed. Second, the survey provides the OEC with a richly detailed set of data for use in the event of a terrorist event or other disaster.



JERT assessments are time- and manpower intensive. Moreover, there have been many assessment requests from the public, including from buildings that, while large, are not considered to be at particularly high risk. The number of requests has far exceeded the capacity of the JERT. In response, the CPD Bomb and Arson Section has initiated a training program that prepares site managers to conduct their own assessments, identify and mitigate vulnerabilities, and collect and submit relevant data to the OEC. The training, designed for groups of 50–100 people, includes multimedia presentations and allows for more efficient use of scarce assessment resources. Both the JERT and self-assessments have created and strengthened partnerships between the city and its home and business owners.



For most ground-based threats, the security measures discussed elsewhere in this documented briefing should provide a very high degree of protection to high-rise buildings. Moreover, the 1993 WTC bombing demonstrated that it is more difficult—for structural reasons—to destroy a high-rise from the bottom than from the top. [10] Threats from the air remain a concern, but their interdiction is largely outside the spectrum of actions available to building owners and the local emergency management community.

Nevertheless, another significant recent policy choice in Chicago was the request—approved by the Federal Aviation Administration (FAA)—to expand the "no-fly zone" over the city to an area significantly larger than that mandated by the FAA immediately after September 11. This expansion was temporary, and the area has since been reduced, but such an approach may be appropriate for certain portions of Los Angeles.

---

[10]Steven Ashley, "When the Twin Towers Fell," *Scientific American*, October 9, 2001.

Indirect Costs of Security: Some Consequences of Closing Pennsylvania Avenue

- **The indirect economic costs of the closure**
  - **Businesses have moved out of the area, lowering sales revenues and property tax values**
  - **Productivity has declined because of longer commute times**
- **The psychological consequences of the closure**
  - **The closure promotes a "bunker mentality"**
  - **Unreasonable analytic weight is placed on the fear of an unlikely attack**

RAND

The portion of Pennsylvania Avenue in front of the White House was closed in May 1995 as a direct result of its perceived vulnerability to a truck bomb in the wake of the attack on the Murrah Federal building in Oklahoma City. The avenue's continued closure has produced unintended economic and psychological consequences, including:[11]

Businesses have moved out of the area—traffic volumes and congestion at key intersections as a result of the need to redirect traffic around the closure have increased overhead costs in terms of delivery and consignment charges. This has, in turn, "encouraged—or compelled—several firms to relocate from the inner downtown area, lowering retail sales and property tax values, which has further impacted on the District's overall revenue base."[12]

There is reduced productivity in businesses in the surrounding area—commute times for employees working in the area around the closure have reduced their overall productivity.

---

[11]All of the indirect costs mentioned herein are adapted from Bruce Hoffman and Peter Chalk, *Security in the Nation's Capital and the Closure of Pennsylvania Avenue: An Assessment*, Santa Monica, Calif.: RAND, DRU-2315-2-FCCDC, 2000.

[12]Ibid., p. 53.

A "bunker mentality" has developed—by closing off the area, businesses and residents feel removed from other parts of the city, including other branches of the government. The lack of continuity in social and economic activity stifles cooperation and growth of business in the area.

Because more weight may be put on fear than on other security considerations, "we risk implementing sweeping policies and making hard security choices (that also prove subsequently hard to reverse) based on misperception and misunderstanding, rather than on hard analysis built on empirical evidence."[13]

Although these consequences cannot and should not be compared directly with the effects of security measures taken at Los Angeles high-rise buildings, they do promote alternative lines of thinking that building owners and security managers should contemplate when making security investment decisions that, like the closure of Pennsylvania Avenue, could have indirect economic consequences for the building, the businesses within it, and the surrounding area.

To illustrate, consider the fact that businesses have moved out of the Washington, D.C., inner-city area because of higher overhead costs. In Los Angeles high-rises, if security costs are passed on to the tenants, they might opt to relocate to another building. The decrease in productivity due to longer commutes can be compared with the decrease in productivity associated with waiting in line for security checks at building entrances. A "bunker mentality" within a specific high-rise might hinder prospective new tenants from choosing to occupy the building. Finally, like the D.C. decisions, which are heavily weighted toward a worst-case scenario, security decisions in Los Angeles high-rises might be skewed toward protecting against something that is highly unlikely. The security measures that might result, such as searches of individuals and/or cars, could produce a level of inconvenience that dissuades people from conducting business in the building.

This, then, is the large challenge faced by owners and occupants of high-rise buildings: What is the proper balance between security and economic vitality? While it is difficult to argue that one should not institute a whole raft of security measures in the wake of 9/11, it is important to be sure some analysis is done to help the cure not become worse than the disease.

---

[13]Ibid., p. 22.

Briefing Outline

- Introduction and Summary Observations
- Key Considerations for Building Security
  - Defining the threats and vulnerabilities
  - Establishing the objectives of security
  - Understanding existing security practices and technologies
  - A context for existing security measures
- Learning from Three Case Studies
  - Lessons learned from 9/11
  - A best case example: Chicago
  - Indirect economic costs: closing Pennsylvania Avenue
- √ Key Planning Considerations for High-Rise Buildings
- Potential Roles for Government
- Recommendations for Los Angeles

RAND

Key Planning Considerations for Los Angeles High-Rise Buildings

- **Fire department–approved emergency plan**
  - **Fire safety inspector must be involved**
  - **Occupant instruction is mandatory**
  - **Floor wardens need to be assigned**
  - **Provisions for emergency evacuation signs are included**
- **Fire drills**
  - **Individual floors must have one annual drill**
  - **Total building evacuation is not required**
- **Assistance for the handicapped**

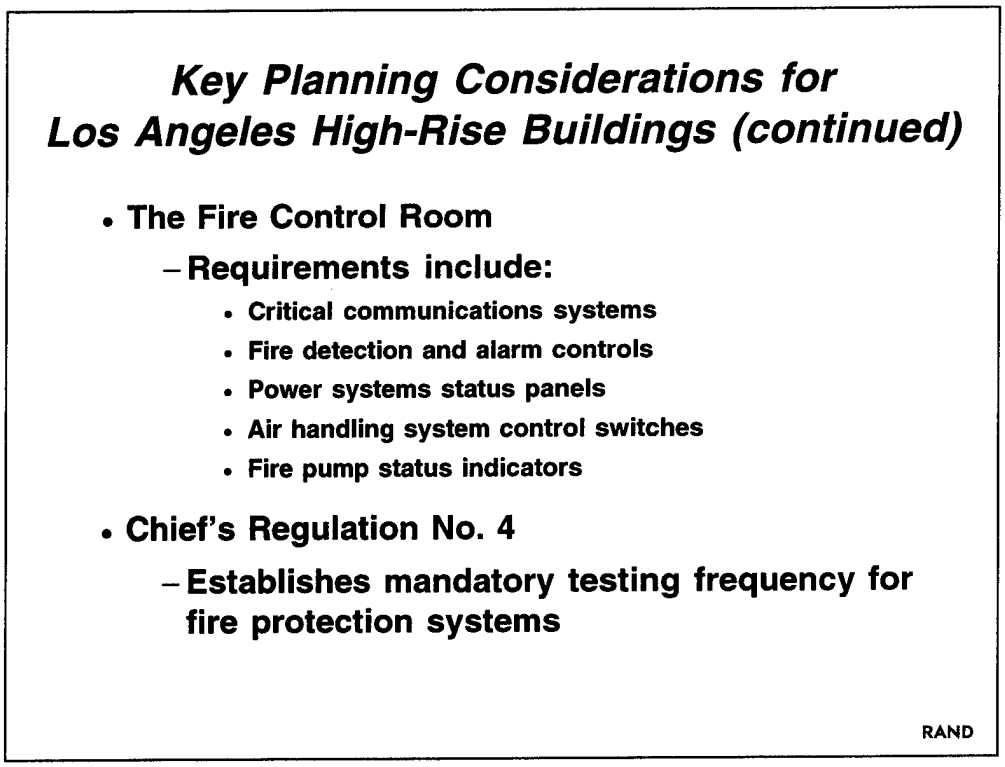
RAND

Chapter V, Article 7, Section 57.33.19 of the Los Angeles City Code specifically covers emergency planning and evacuation requirements for high-rise buildings. According to this section, high-rise buildings are required to have a detailed emergency plan approved by the Los Angeles Fire Department (LAFD) Fire Safety Education Unit. The plan must include the assignment of a fire safety director, provisions for instructing building occupants on emergency procedures, the designation of floor wardens, and the preparation of emergency exit plans, procedures, and evacuation signs.

All major high-rise buildings in Los Angeles have such plans, but there are different philosophies regarding the types of personnel selected to serve as wardens and the methods of communication to occupants.

Annual fire drills are mandatory for individual high-rise floors and must be documented by the fire safety director. Total building evacuation is not required by current regulations.

The fire safety director must maintain a current list of persons needing special evacuation assistance and the kind of assistance needed.



New high-rise buildings must have a fire control room near the building's main entrance. The Los Angeles City Code (Chapter V, Article 7, Section 57.118.02) details the minimum size, fire resistance requirements, and necessary equipment and controls for the fire control room. Some elevator and fire control rooms located near entrances could represent a vulnerability, and there is a trade-off between easy access for responders and security and for easy access by perpetrators. Both the LAFD and building owners and managers will want to review the fire control room locations and protocols as part of updated plans for building emergency preparedness.

LAFD Chief's Regulation Number 4 establishes mandatory testing and inspection frequency for fire protection equipment. LAFD has established the Chief's Regulation No. 4 Unit within the Bureau of Fire Prevention and Public Safety specifically to assist in this process. The unit maintains a list of currently certified testers of fire protection equipment and can answer any other questions about the regulation. As examples, high-rise emergency generator and lighting systems and high-rise fire doors must be tested annually. Booster pump Class H standpipe systems must be tested biannually.

Los Angeles Policy Changes

- There have been no formal changes made to high-rise policies
- WTC evacuation was largely successful
- These topics are under review:
  - Acceptable use of unaffected elevators
  - Frequency/extent of evacuation drills

RAND

In Los Angeles, there have been very few legal or government policy changes in terms of requirements for planning for high-rise disasters since September 11. This is not necessarily a bad thing. Buildings in California are already subject to long-existing, stringent codes enacted to ensure earthquake survivability. As noted above, evacuation plans have also been developed according to federal, state, and local guidelines and must be approved by the LAFD Fire Safety and Education Unit. Local planning guidelines are not substantively different from those that were in place in the WTC, and that are discussed in commonly available publications such as FEMA's report, *Emergency Management Guide for Business and Industry*.[14]

Nevertheless, many guidelines are being reconsidered in the wake of September 11. One, for example, is the possible use of unaffected elevators for evacuation. Currently, elevators generally are automatically recalled (to the ground floor) when a fire alarm is activated. Another is the the frequency and extent of evacuation drills. Previously, since all high-rise fires were limited in their scope (i.e., no high-rise fire ever destroyed an entire building) planned

[14]Available at the FEMA web site: www.fema.gov/.

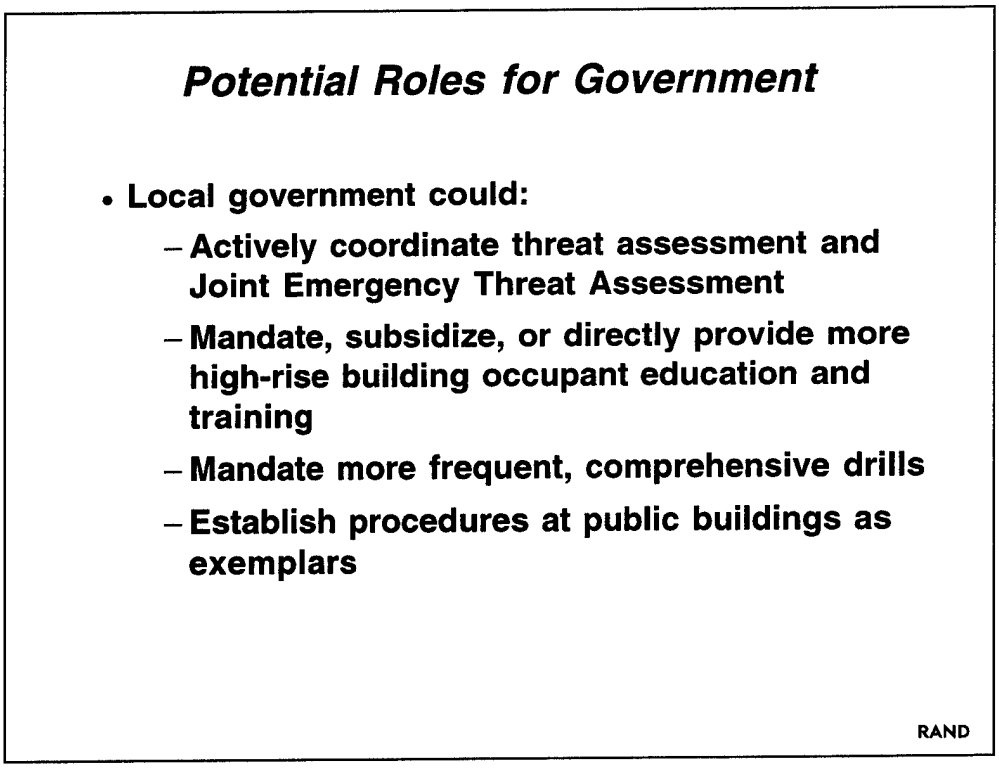
evacuations were to include only the affected floors with buffers above and below. Now, plans are being considered to include possible full building evacuations.

There likely will be reviews of building design specifications as the various studies of the World Trade Center and Pentagon bombings develop technical findings about what happened to the structures.

Briefing Outline

- Introduction and Summary Observations
- Key Considerations for Building Security
  - Defining the threats and vulnerabilities
  - Establishing the objectives of security
  - Understanding existing security practices and technologies
  - A context for existing security measures
- Learning from Three Case Studies
  - Lessons learned from 9/11
  - A best case example: Chicago
  - Indirect economic costs: closing Pennsylvania Avenue
- Key Planning Considerations for High-Rise Buildings
- √ Potential Roles for Government
- Recommendations for Los Angeles

RAND



Government can improve public policy by establishing clear, well-articulated means for threat assessment and sharing the threat assessment burden across multiple agencies, much in the same fashion as Los Angeles has done for response to the earthquake "threat." Chicago has shown that this approach can be effective, although admittedly time-consuming and expensive. The Los Angeles Police Department has completed a risk assessment process, the Terrorism Early Warning Group (TEWG) has begun to develop target folders, and the Los Angeles County Sheriff has established general coordination procedures, among other actions that have been taken in the region and the state. Los Angeles should consider a mechanism for coordinating and sharing the specific threat assessment process that preserves the privacy needed for public law enforcement officers but embraces the needs of the private sector, especially owners and occupants of high-rise buildings that may be at risk.

Government should also consider a range of options for encouraging training and education for high-rise building occupants and vendors. At one end of the spectrum, some training (or certification programs) could be mandated but be provided wholly by the private sector. At the other end, Los Angeles could increase the amount of education and training it provides as a public service. Somewhere in the

middle are a range of subsidies and incentive programs that could be put in place to encourage enhanced training.

Although fire drills are a burden and certainly carry economic costs, Los Angeles should consider more frequent drills for response to emergency situations in high-rise buildings. We cannot stress often enough that a well-drilled population in a high-rise building significantly increases their safety in the face of an incident. A task force of private-sector stakeholders, public safety officials, and elected officials may be a useful approach to developing new standards that balance the life safety and economic issues of increased drilling.

Finally, Los Angeles may want to create an interdepartmental group to evaluate and recommend exemplary security practices for public buildings. Public buildings have an inherently higher need for open access, but many also have stringent security requirements. Currently, it is not clear that public buildings in Los Angeles represent the best security practices or the best balance of life safety and economic considerations. Government may want to take the lead by setting a good example.

Private security is a major industry in the state and region and is destined to grow in the wake of 9/11. If the trend of outsourcing many support functions continues and expectations for performance of security forces continue to rise, it may be appropriate for Los Angeles to establish some standards of education, training, and retraining for private security officers. There may also be a public role for helping to define and promulgate appropriate guidelines for the training and operation of private security forces. While it is inappropriate to take the steps the federal government has taken with airport security forces, it may well be appropriate to work with the private sector to generate new standards of qualifications, training, and acceptable private security practices. In addition, there clearly is a possible leadership role for government as part of its responsibility for the public health and safety. Helping the community identify best security standards and practices and then seeing that those practices are followed consistently are roles local government may want to consider.

Also, just as the idea of the "trusted traveler" is gaining some credibility as one part of a broader program for speeding security checks at airports, there may be an analogy for vendors and others who supply high-rise buildings in Los Angeles. Because any program that involves personal information has civil liberty issues,

local government may be an excellent place to coordinate the development of standards for introducing similar access programs in Los Angeles high-rise buildings.

Perhaps one of the most difficult areas for achieving solid improvement is the sharing of threat information and information regarding suspicious activity. Elsewhere we suggest that part of a "layering" strategy of security must involve building occupants in some fashion. But indiscriminate identification and sharing can be as dangerous to society in the long run as none at all. Also, for good reasons, law enforcement officials have concerns about sharing information. In both instances, the public sector may be a home for leadership in improving guidelines and communication channels for sharing localized threat information.

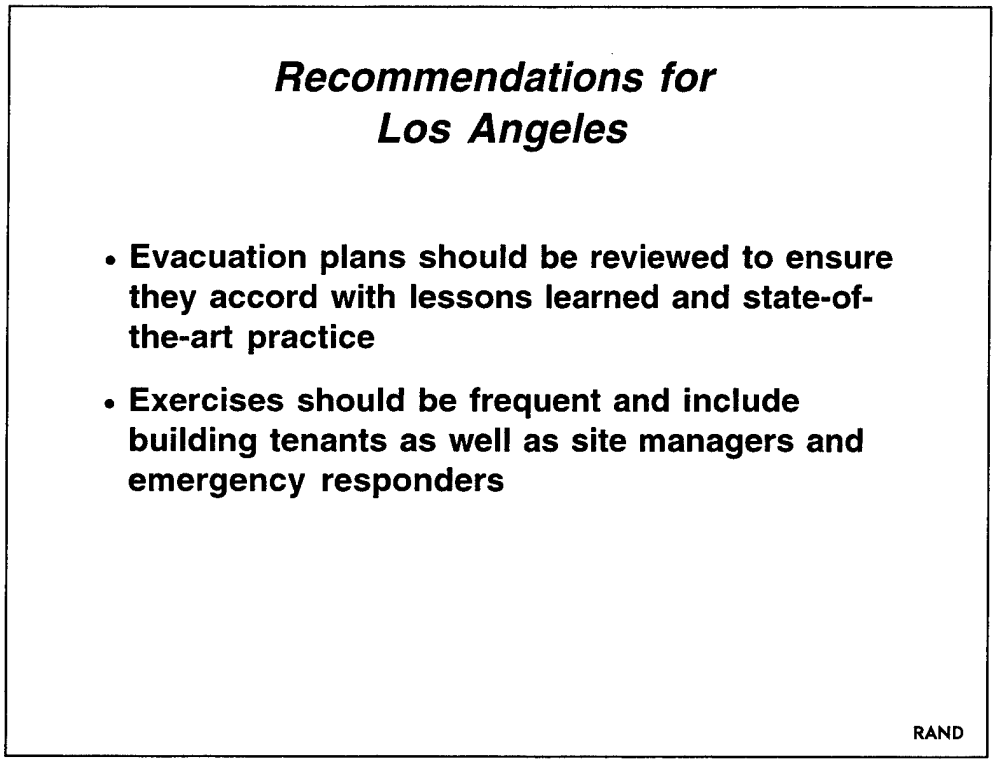
Finally, if, as we believe, a heightened level of security likely will be exercised well into the future, it would be very helpful to have more scientific research and evaluation, including pilot programs, of security technology and practices. Perhaps something similar to the formula used for funding arts programs (e.g., "1% for the arts") should be considered to fund improved research and development in the security area.

Briefing Outline

- Introduction and Summary Observations
- Key Considerations for Building Security
  - Defining the threats and vulnerabilities
  - Establishing the objectives of security
  - Understanding existing security practices and technologies
  - A context for existing security measures
- Learning from Three Case Studies
  - Lessons learned from 9/11
  - A best case example: Chicago
  - Indirect economic costs: closing Pennsylvania Avenue
- Key Planning Considerations for High-Rise Buildings
- Potential Roles for Government

√ Recommendations for Los Angeles

RAND



It is unreasonable to expect a high-rise building to survive a strike of the magnitude of those sustained by the WTC. The obvious, and best, preparation for such an attack is to prevent it from happening. However, even a far smaller strike, like that in Oklahoma City, would have the potential to exact a tremendous cost in both life and property. In Los Angeles, standards for evacuation plans, including exercise schedules, and for relevant building infrastructure should be continually reviewed and updated where necessary to reflect the current state of the art. At the WTC itself, lessons learned from the terrorist attack in 1993 led to over $90 million of building improvements, including the installation of sprinkler systems, redundant power and lighting systems, evacuation chairs for the disabled, reflective paint on evacuation routes, and duplicate fire-control command posts. Exercises should be taken seriously and conducted frequently. Exercise participation should not be limited to building tenants. Local responders must also take part in a given building's exercise regime, particularly for high-risk locations. The most important lesson learned from September 11: Successful evacuation saved thousands of lives.

The Building Owners and Managers Association Security and Emergency Preparedness Committee may want to undertake a more formal sharing of standards and practices and take the lead in organizing exercises with local responders, as well as with building occupants.

Recommendations for Los Angeles (continued)

- **Conduct and regularly update threat and vulnerability assessments**
- **Emphasize response**
  - **Firmly establish protocols**
  - **Conduct more frequent and realistic drills**
- **Educate tenants about their roles**
  - **Tenants have to be aware and active**

RAND

With a general understanding of the role of security and the state of security, some suggestions can be made.

First, JERT-type assessments of each building should be performed so that those who make building security decisions can better understand the building's particular vulnerabilities given the nature of the threat. If JERT-type assessments cannot be accomplished, then training similar to that given in Chicago should be offered to enable security directors to make self-assessments.

Second, recognizing that some attacks cannot be prevented—it is very difficult to stop a motivated attacker from doing that which he is willing to sacrifice himself to do—more emphasis should be placed on response. Response protocols and the events that trigger them must be firmly established. There should be formal mechanisms for communicating with tenants exactly what is required of them and under what circumstances. The protocols should be tested more often than annually and under more realistic scenarios, suggesting that some drills might best occur without warning and that participation be mandatory.

Third, there must be a greater emphasis placed on tenants being partly responsible for their own security. Tenants must be educated about the role they can play and how they can best perform that role.

The Building Owners and Managers Association Committee on Security and Emergency Preparedness may want to consider taking a lead role in identifying appropriate training materials and courses and developing appropriate exercise scenarios specific to Los Angeles.

Recommendations for Los Angeles (continued)

- **Formulate Target Folders/Emergency Plans**
  - **Unification, standardization, and computerization of data would be beneficial**
  - **Building managers and beat-level officers and firefighters should be used**
  - **Building owners/managers should consider why their building would be specifically targeted**
  - **Buildings owners/managers should consider having a representative in the LA County TEWG**

RAND

The Los Angeles County TEWG, headquartered at the Los Angeles County Sheriff's Department Emergency Operations Center, has begun creating detailed target folders for a number of high-profile targets in Los Angeles County. Files of this type have already proven their value in Los Angeles and elsewhere in the United States and around the world in a variety of emergency situations, of which terrorism is but one. Currently, while the LAFD maintains copies of high-rise evacuation plans, they are distinct from TEWG target folders. There are currently no target folders for high-rise buildings in Los Angeles.

As in the Chicago example, building owners can and should play a major role in the folders' development and currency. Providing the data in a standard, electronic format would allow for their rapid update and transmission among relevant agencies and to suitably equipped field units. The ability for responders to download floor plans, etc. while at or en route to an incident would be of obvious and substantial benefit. The TEWG is a relatively small organization. Making use of the relevant beat officers in Los Angeles County, at least for initial site data collection and assessment, could be a useful step toward the creation of a comprehensive city- or county-wide unified target folder library.

As part of the overall effort of incident prevention and effect mitigation, building owners and managers should address the problem by investigating the specific characteristics of their building that make them a likely target. Understanding the type of perpetrator of a particular type of crime or attack can assist in measuring the likelihood of an event occurring. This assessment will also assist in developing countermeasures, indicators and warnings, and customized responses to a particular, most likely kind of event.

Regular communication between building owners/managers and law enforcement organizations should be formalized. Periodic attendance at the TEWG meetings could maintain a dialogue between building owners and law enforcement organizations. This regular communication could serve mutually beneficial goals, such as: building owner/manager understanding of law enforcement/first-responder protocols and standard operating procedures, possible development of site-specific exercises, the establishment of complete and useful target folders, mutual assistance in identifying indicators and warnings of a potential attack, and ongoing communication that ensures each group is kept up-to-date on relevant data and practices.

Recommendations for Los Angeles (continued)

- **Low-tech means can provide subtle, yet reliable effects**
  - **Landscaping can be used for security**
  - **Procedural measures add a thinking component to security**
- **High-tech measures provide obvious deterrence**
- **The perception of safety derived from technology might help secure building occupancy**

RAND

The open area surrounding a high-rise can be landscaped with security in mind. For instance, shrubbery can be planted in locations that block or channel people and automobiles into desired locations. Cactus and bougainvillea-type plants can be inserted in locations to prevent approach. Benches and other furniture elements can also be part of a security plan. There is a growing cadre of architects in the country who are developing approaches to security, especially perimeter security, that are friendly to building users, but still meet security needs.

Security personnel can be trained to better identify potential threats. Beyond the physical means of weapons detection devices, security personnel should learn to identify potential threats through surveillance and questioning techniques. Similar to the simple, subtle questions asked by customs officials at airports, security questions can be developed for building security personnel to ensure that building visitors are more effectively screened before entering. These techniques can be developed with law enforcement officials of the L.A. County TEWG. The obvious advantage of this approach is the relatively low cost in implementing such measures.

High-technology solutions to threat identification provide both deterrence and reassurance capabilities. Potential threats, realizing the hurdles they must overcome to enter a building protected with

high-technology surveillance and protection measures, might opt for a less secure target. Building occupants, aware of the obvious safety measures in place, will most likely appreciate the security provided and potentially maintain a longer-term tenancy.